Processor Privacy Rules

Contact details

Philips Privacy Office
c/o Philips International BV, Amstelplein 2, 1096 BC, the Netherlands.
E-mail: Philips_Privacy_Office@philips.com

The most recent online version of the Processor Privacy Rules for BCI Data can be found on internet:
http://www.philips.com/shared/assets/Investor_relations/pdf/businessprinciples/Philips_Processor_Rules.pdf

Version history

Date	*Updated sections*	*Version*
17 June 2011	Final version	1.0
20 July 2011	Final version, typo's fixed, added Annex 2	1.1

14 September 2012	New version pursuant to WP195	1.2
19 June 2013	New version incorporating comments Dutch DPA	1.3
19 December 2013	New version incorporating comments UK and Polish DPA	1.4
16 July 2015	Final version (typo's fixed)	2.0

Introduction

Philips provides processing services to its business customers involving personal data processed by such customers in the course of performing their business activities. Philips processes such personal data as a Data Processor on behalf of these business customers.

The General Business Principles of Philips express our commitment to strive to protect personal data. These Processor Privacy Rules indicate how this commitment shall be implemented. For the privacy rules applicable to the processing of customer data by Philips in its role as a Data Controller, refer to the *Privacy Rules for Customer, Supplier and Business Partner Data*.

Article 1 – Scope, Applicability and Implementation

Scope *Philips as Data Processor*	**1.1**	These Rules address the worldwide Processing of Personal Data of individual customers or employees of Business Customers (**Business Customer's Individuals Personal Data or BCI Data**) by Philips in its role as a Data Processor in the course of delivering Customer Services.
Processing in non- Adequate Country	**1.2**	These Rules apply to BCI Data that are: (i) subject to Data Transfer Restrictions; and (ii) Processed by Philips in a non-Adequate Country.
Electronic and paper-based Processing	**1.3**	These Rules apply to the Processing of BCI Data by electronic means and in systematically accessible paper-based filing systems.
Applicability of local law and these Rules	**1.4**	Business Customer's Individuals keep any rights and remedies they may have under applicable local law. Where these Rules provide more protection than applicable local law or provide additional safeguards, rights or remedies for Business Customer's Individuals, these Rules shall apply.

Sub-policies and notices	**1.5**	Philips may supplement these Rules through sub-policies and notices that are consistent with these Rules.
Compliance Responsibility	**1.6**	These Rules are binding on Philips. The **Responsible Executive** shall be accountable for her business organization's compliance with these Rules. Philips Staff must comply with these Rules.
Effective date	**1.7**	These Rules enter into force as of 16 July 2015 **(Effective Date)**. They are published on the Philips General Business Principles Internet site, except that the description of the security measures may be replaced by a summary description.
Rules supersede prior policies	**1.8**	These Rules supersede all Philips privacy policies that exist on the Effective Date to the extent they address the same issues or conflict with the provisions of these Rules.
Implementation	**1.9**	These Rules shall be implemented within Philips based on the timeframes specified in Article 15.
Role of Philips International	**1.10**	KPENV has tasked Philips International with the coordination and implementation of these Rules.
Privacy Officer Advice	**1.11**	Where there is a question as to the applicability of these Rules, Staff shall seek the advice of the appropriate Privacy Officer prior to the relevant Processing.

Article 2 – Business Customer Service Contract

Business Customer Service Contract	**2.1**	Philips shall Process BCI Data only on the basis of a written contract with a Business Customer (**Business Customer Service Contract**). The Philips Contracting Entity uses Sub-Processors, both Philips Sub-Processors and Third Party Sub-Processors, in the regular performance of Business Customer Service Contracts. The standard Business Customer Service Contract shall authorize the use of such Sub-Processors, provided that the Philips Contracting Entity remains liable to the Business Customer for the performance of the contract by the Sub-Processors. If the Business Customer Service Contract explicitly does not authorize the use of Sub-Processors, Article 7 shall not apply.

Termination Business Customer Service Contract	**2.2**	Upon termination of the Business Customer Service Contract, Philips shall, at the option of the Business Customer, return the BCI Data and copies thereof to the Business Customer or shall securely destroy such BCI Data and certify to the Business Customer that Philips has done so, except to the extent the Business Customer Service Contract or applicable law provides otherwise. In that case, Philips shall no longer Process the BCI Data, except to the extent required by the Business Customer Service Contract or applicable law.
Audit of termination measures	**2.3**	Philips shall, at the request of the Business Customer or Relevant Data Protection Authority, allow its Processing facilities to be audited in accordance with Article 10.2 or 10.3 (as applicable) to verify that Philips has complied with its obligations under Article 2.2.

Article 3 – Compliance Obligations Philips

Instructions of the Data Controller	**3.1**	Philips shall Process BCI Data only on behalf of the Business Customer and in accordance with any instructions received from the Business Customer.
Compliance with Applicable Adequate Data Protection Law	**3.2**	Philips shall Process BCI Data only in accordance with the Applicable Adequate Data Protection Law and shall deal promptly and appropriately with requests for assistance of the Business Customer to ensure compliance of the Processing of the BCI Data with the applicable Adequate Data Protection Law.
Notification of non-compliance, substantial adverse effect	**3.3**	If Philips: (i) determines that it is unable for any reason to comply with its obligations under Article 3.1 and 3.2 and Philips cannot cure this inability to comply; or (ii) becomes aware of any circumstance or change in the Applicable Data Processor Law, except with respect to the Mandatory Requirements, that is likely to have a substantial adverse effect on Philips ability to meet its obligations under Article 3.1, 3.2 or 10.3; Philips shall promptly notify the Business Customer thereof, in which case the Business Customer will have the right to temporarily suspend the Processing until such time the Processing is adjusted in such a manner that the non-compliance is remedied. To the extent such adjustment is not possible, the Business Customer shall have the right to terminate the relevant part of the Processing by Philips.

Request for disclosure of BCI Data	**3.4**	Philips shall promptly notify the Business Customer of any legally binding request Philips receives for disclosure of BCI Data by a law enforcement authority unless otherwise prohibited by law from making such disclosure.
Inquiries of the Business Customer	**3.5**	Philips shall deal promptly and appropriately with inquiries of the Business Customer related to the Processing of the BCI Data pursuant to the terms of the Business Customer Service Contract.

Article 4 – Processor Purposes

Legitimate Business Purposes

4.1 Where Philips serves as a Data Processor, Personal Data and Sensitive Data may be Processed by Philips for one or more of the following purposes**:**

(i) **Customer data management information technology services** including:
- (a) hosting, storage, backup, or archiving;
- (b) reporting on the use of data services by a Customer;
- (c) security maintenance (e.g., implementing access controls, auditing use, managing servers, managing network security, managing incidents); or
- (d) account management of third-party use of Customer-specific Philips products or services (e.g., use reporting and billing of a Customer's customer on behalf of the Customer).

(ii) **Customer support services** including:
- (a) providing (local and remote) assistance to Customer in the use or repair of Philips products or services;
- (b) Philips generation of service level reports or other reports on a Customer's use of Philips products or services for Customer management information purposes; or
- (c) life-cycle management of Philips products and services (e.g., planning, evaluation, demonstration, installation, calibration, training, maintenance, decommissioning) to facilitate continued and sustained use by a Customer of Philips products and services.

(iii) **Customer-specific custom services** including:
- (a) device or system tuning for the purpose of adjusting the service or product to meet a Customer's

specifications (e.g., by engaging application specialists, undertaking project management activities, modifying of device or system);

(b) the collection and analysis of Customer use data to report trends (e.g., specific status reports, management reporting, proactive management for security, the general improvement of Customer's internal operations);

(c) the purchase of goods and services on behalf of a Customer (e.g., contract broadband network service for device placement and data acquisition, third-party hardware integration); or

(d) the provision of training for Customer's staff or third parties (e.g., equipment training, HIPAA training, infection control training, radiation training).

(iv) **Philips internal business process execution and management** leading to incidental Processing of Personal Data or Sensitive Data for:

(a) internal auditing of Philips Processor-related activities;

(b) activities related to compliance with applicable law or regulation (e.g., data processing law, medical device regulation);

(c) data deidentification and aggregation of deidentified data for data minimization; and

(d) use of deidentified, aggregate data to facilitate continuity, sustainability, and improvement of Philips products and services.

Article 5 – Security Requirements

Data security	**5.1**	Philips shall take appropriate, commercially reasonable, technical, physical and organizational measures to protect BCI Data from misuse or accidental, unlawful or unauthorized destruction, loss, alteration, disclosure, acquisition or access during the Processing. Philips shall in any event take the measures specified in Annex 2 of these Rules, which Annex shall be revised by Philips if so required to reflect industry standards, or such stricter measures as instructed by the Business Customer in the Business Customer Service Contract.
Data access and confidentiality	**5.2**	Philips shall provide Philips Staff access to BCI Data only to the extent necessary to perform the Processing. Philips shall impose confidentiality obligations on Staff that has access to BCI Data.
Data Security Breach notification requirement	**5.3**	Philips shall notify the Business Customer of a Data Security Breach as soon as reasonably possible following discovery of such breach, unless a law enforcement official or supervisory authority determines that notification would impede a (criminal) investigation or cause damage to national security or the trust in the relevant industry sector. In this case, notification shall be delayed as instructed by such law enforcement official or supervisory authority. Philips shall respond promptly to inquiries of the Business Customer relating to such Data Security Breach.

Article 6 – Transparency to Business Customer's Individuals

Copy of Data Protection Provisions of Business Customer Service Contract	**6.1**	Philips shall provide the Business Customer's Individual, at its request, the contact details of the relevant Business Customer. If the Business Customer's Individual is unable to obtain from the Business Customer a copy of the data protection provisions of the relevant Business Customer Service Contract, Philips shall provide the Business Customer's Individual with a copy of these provisions. Where the disclosure sets forth a description of detailed security measures, Philips may replace the details with a summary description.
Other Requests of Business Customer's Individuals	**6.2**	Philips shall promptly notify the Business Customer of requests (other than requests under Article 6.1) or complaints that are received directly from a Business Customer's Individual without responding to such requests or complaints, unless otherwise instructed by the Business Customer in the Business Customer Service Contract. If instructed by the Business Customer to respond to requests and complaints of Business Customer's Individuals, Philips shall ensure that the Business Customer's Individual is provided with all required information (including the point of contact and the procedure) in order for the Business Customer's Individual to be able to effectively make the request or lodge the complaint.

Article 7 – Sub-Processors

Third Party Sub-Processing Contracts	**7.1**	Third Party Sub-Processors may Process Business Customer Data only if the Third Party Sub-Processor has a written contract with Philips. The contract shall impose similar data protection-related Processing terms on the Third Party Sub-Processor as those imposed on the Philips Contracting Entity by the Business Customer Service Contract and these Rules.
Publication of Overview of Sub-Processors	**7.2**	Philips shall publish on the appropriate Philips website an overview of the categories of Sub-Processors (both Third Parties and Philips Group Companies) Philips involves in the performance of the relevant Customer Services. This overview shall be promptly updated in case of changes.

Article 8 – Supervision and compliance

Chief Privacy Officer	**8.1**	Philips International shall appoint a Chief Privacy Officer who is responsible for: (i) supervising compliance with these Rules; (ii) providing periodic reports, as appropriate, to the Chief Legal Officer on data protection risks and compliance issues; and (iii) coordinating, in conjunction with the appropriate Senior Privacy Officers, official investigations or inquiries into the Processing of BCI Data by a public authority.
Privacy Council	**8.2**	The Chief Privacy Officer shall establish an advisory Privacy Council. The Privacy Council shall create and maintain a Philips framework for: (i) the development of the policies, procedures and system information (as required by Article 9); (ii) planning training and awareness programs; (iii) monitoring and reporting on compliance with these Rules; (iv) collecting, investigating and resolving privacy inquiries, concerns and complaints; and (v) determining and updating appropriate sanctions for violations of these Rules (e.g., disciplinary standards).
Senior Privacy Officers	**8.3**	All of the Sector Privacy Officers, Country Privacy Officers, Region Privacy Officers and Function Privacy Officers are considered Senior Privacy Officers. Senior Privacy Officers will be designated as follows: • each Sector shall designate a Sector Privacy Officer; • each Country shall designate a Country Privacy Officer, unless the Chief Privacy Officer determines that certain Countries will be grouped into a Region, in which case the Region will designate a Region Privacy Officer; • the Chief Privacy Officer shall determine for which Functions a Function Privacy Officer is appropriate, after which the respective Function shall designate a Function Privacy Officer; • the Chief Privacy Officer shall act as the Senior Privacy Officer for those Functions for which no Function Privacy Officer is designated; and • all Senior Privacy Officers shall be published on the Philips intranetsite (pww.privacy.philips.com). These Senior Privacy Officers may, in turn, establish a network of qualified Privacy Officers sufficient to direct compliance with these Rules within their respective organizations. Reference to the appropriate privacy officers shall be made in the relevant

		privacy notices. These Senior Privacy Officers shall perform at least the following tasks: (i) regularly advise their respective executive teams and the Chief Privacy Officer on privacy risks and compliance issues; (ii) maintain (or ensure access to) an inventory of the system information for all systems and processes that Process BCI Data (as required by article 9.2); (iii) implement the privacy compliance framework as required by the Chief Privacy Officer; (iv) be available for requests for privacy approval or advice and direct the requests to the appropriate Privacy Officer(s) (i.e., Privacy Officer(s) whose organizations are impacted by the approval or advice); (v) own and authorize all appropriate privacy sub-policies in their organizations; and (vi) cooperate with the Chief Privacy Officer, other Senior Privacy Officers, the Privacy Officers, and the General Business Principles Compliance Officers.
Responsible Executive	**8.4**	The Responsible Executive shall perform at least the following tasks: (i) ensure that the policies and procedures are implemented and the system information is maintained (as required by Article 9); (ii) provide such system information to the Senior Privacy Officers necessary as required for her to comply with the task listed in Article 8.3 sub (ii); (iii) ensure that Personal Data are returned or securely deleted or destroyed after termination of the Business Customer Service Contract (as required by Article 2.2); (iv) determine how to comply with the Rules when there is a conflict with applicable law (as required by Article 13.1); and (iii) inform the appropriate Senior Privacy Officers of any new legal requirement that may interfere with Philips ability to comply with these Rules (as required by Article 13.2).
Default Privacy Officer	**8.5**	If no Senior Privacy Officer has been designated in a Sector, Country or Region, the designated compliance officer for the Philips General Business Principles for the relevant Philips Group Company is responsible for supervising compliance with these Rules.
Privacy Officers	**8.6**	Where a Privacy Officer holds her position pursuant to law, she

with statutory position		shall carry out her job responsibilities to the extent they do not conflict with her statutory position.

Article 9 – Policies, procedures and training

Policies and procedures	**9.1**	Philips shall develop and implement policies and procedures to comply with these Rules.
System information	**9.2**	Philips shall maintain readily available information regarding the structure and functioning of all systems and processes that Process BCI Data (e.g., inventory of systems and processes, privacy impact assessments).
Staff training	**9.3**	Philips shall provide training on these Rules and other privacy and data security obligations to Staff who have access to or responsibilities associated with managing BCI Data.

Article 10 – Monitoring compliance

Internal audits	**10.1**	Philips Internal Audit shall audit business processes and procedures that involve the Processing of BCI Data for compliance with these Rules. The audits shall be carried out in the course of the regular activities of Philips Internal Audit or at the request of the Chief or a Senior Privacy Officer. The Chief Privacy Officer may request to have an audit as specified in this Article conducted by an external auditor. Applicable professional standards of independence, integrity and confidentiality shall be observed when conducting an audit. The Chief Privacy Officer and the appropriate Senior Privacy Officers shall be informed of the results of the audits. In case the audit identifies violations of the Rules, these will be reported to senior management. A copy of the audit results will be provided to the Dutch Data Protection Authority upon request.

Business Customer audit

10.2 Philips shall, at its option, either:

(i) make the facilities it uses for the Processing of BCI Data available for an audit by the Business Customer or a qualified independent third party assessor selected by the Business Customer and reasonably acceptable to Philips (in which case the Business Customer shall provide a copy of the audit report to the Chief Privacy Officer), or

(ii) Philips shall provide to the Business Customer a statement issued by a qualified independent third party assessor certifying that the Philips business processes and procedures that involve the Processing of BCI Data comply with these Rules.

Audit by Relevant Data Protection Authority

10.3 A Relevant Data Protection Authority may request an audit of the facilities used by Philips for the Processing subject to the same conditions (regarding the existence of the right to audit, scope, subject and other requirements) as would apply to an audit by that Data Protection Authority of the Business Customer itself under the Applicable Data Controller Law.

Annual Report

10.4 The Chief Privacy Officer shall produce an annual BCI Data protection report for the Chief Legal Officer on Philips' compliance with these Rules and other relevant issues.

Mitigation

10.5 Philips shall, if so indicated, ensure that adequate steps are taken to address breaches of these Rules identified during the monitoring or auditing of compliance pursuant to this Article 10.

Article 11 – Legal issues

Specific provision when Data Protection Authorities in EEA have jurisdiction under national law

11.1 If a Data Protection Authority of one of the EEA countries has jurisdiction under its applicable data protection law to evaluate data transfers by a Group Company established in its country, such Data Protection Authority may evaluate these data transfers also against these Rules. The Dutch Data Protection Authority will provide cooperation and assistance where required, including providing audit reports available at the Dutch Data Protection Authority insofar as relevant to evaluate the aforementioned data transfers against these Rules.

Rights of Business Customer's Individuals

11.2 When the Business Customer has factually disappeared or ceased to exist in law or has become insolvent, unless a successor entity has assumed the legal obligations of the Business Customer by contract or by operation of law (in which

case the Business Customer's Individual should enforce its rights against such successor entity), the Business Customer's Individual can enforce against the Philips Contracting Entity Article 3, 5.1, 5.3, 6, 7.1, 7.2, 10.3, 11.1, 11.2, 11.4, and any claim for direct damages as a result of a breach of these enumerated provisions.

To the extent the Business Customer's Individual may enforce any rights against the Philips Contracting Entity, the Philips Contracting Entity may not rely on a breach by a Sub-processor of its obligations to avoid liability. Philips may, however, assert any defenses that would have been available to the Business Customer.

Jurisdiction for Claims of Business Customer's Individuals

11.3 The Business Customer's Individual may, at her choice, submit any claim she has under Article 11.2 against the Philips Contracting Entity:

(i) to mediation by;

(a) an independent person located in the country in which the Business Customer's Individual resides or, if the Business Customer's Individual does not reside in an EEA Country, an independent person located in the Netherlands; or

(b) a Relevant Data Protection Authority;

(ii) to the courts in the country of establishment of the Business Customer or, if the Business Customer is not established in an EEA Country, to

a court in the Netherlands but in that case only against Philips International; or

(iii) to a Relevant Data Protection Authority or, if the Business Customer is not established in an EEA Country, to the Dutch Data Protection Authority, but in that case only against Philips International.

The courts, the Relevant Data Protection Authority and the Dutch Data Protection Authority shall apply their own substantive and procedural laws to the dispute. Any choice made by the Business Customer's Individual will not prejudice the substantive or procedural rights he may have under applicable law.

Rights of Business Customers

11.4 The Business Customer may enforce these Rules against the Philips Contracting Entity or, if the Philips Contracting Entity is not established in an EEA Country, against Philips International. Philips International shall, if so indicated, ensure that adequate steps are taken to address violations of these Rules by the Philips Contracting Entity or any other Group Company.

The Philips Contracting Entity or Philips International may not

rely on a breach by another Group Company or a Sub-processor of its obligations to avoid liability.

Available remedies, limitation of damages, burden of proof re. damages for Business Customer's Individuals

11.5 In case of a violation of these Rules, Business Customer's Individuals shall be entitled to compensation of damages. However, the Philips Contracting Entity or Philips International shall be liable only for direct damages (which, excludes, without limitation, lost profits or revenue, lost turnover, cost of capital, and downtime cost) suffered by a Business Customer's Individual resulting from a violation of these Rules.

Regarding the burden of proof in respect of damages, it will be for the Business Customer's Individual to demonstrate that she has suffered damage and to establish facts which show it is plausible that the damage has occurred because of a violation of these Rules. It will subsequently be for the Philips Contracting Entity or Philips International to prove that the damages suffered by the Business Customer's Individual due to a violation of these Rules are not attributable to a Group Company or a Sub-processor.

Available remedies, limitation of damages, burden of proof re. damages for Business Customers

11.6 In case of a violation of these Rules, Business Customers shall be entitled to compensation of damages. However, the Philips Contracting Entity or Philips International shall be liable only for direct damages (which, excludes, without limitation, lost profits or revenue, lost turnover, cost of capital, and downtime cost) suffered by a Business Customer resulting from a violation of these Rules.

Mutual assistance Group Companies and redress

11.7 All Group Companies shall cooperate and assist each other to the extent reasonably possible to achieve compliance with these Rules, including an audit or inquiry by the Business Customer or a Relevant Data Protection Authority.

The Philips Group Company upon receiving a request for information pursuant to Article 6.1 or a claim pursuant to Article 11.1, is responsible for handling any communication with the Business Customer's Individual regarding her request or claim except where circumstances dictate otherwise and as mutually agreed among Senior Privacy Officers relevant to the specific issue.

The Philips Group Company that is responsible for the Processing to which the request or claim relates, shall bear all costs involved and reimburse any costs made by other Philips Group Companies in respect thereof.

Advice by Relevant Data Protection Authority

11.8 Philips shall abide by the advice of a Relevant Data Protection Authority with regard to the Processing of BCI Data.

Article 12 – Sanctions for non-compliance

Non-compliance

12.1 Non-compliance of Philips employees with these Rules may result in disciplinary action up to and including termination of employment.

Article 13 – Conflicts between the Rules and Applicable Data Processor Law

Conflict between Rules and law

13.1 Where there is a conflict between Applicable Data Processor Law and the Rules, the relevant Responsible Executive shall consult with the appropriate Senior Privacy Officers and their legal departments to determine how to comply with these Rules and resolve the conflict to the extent reasonably practicable given the legal requirements applicable to the relevant Group Company.

New conflicting legal requirements

13.2 The relevant Responsible Executive, in consultation with her legal department, shall promptly inform the appropriate Senior Privacy Officers of any new legal requirement that may interfere with Philips ability to comply with these Rules.

Article 14 – Changes to the Rules

14.1 Any changes to these Rules require the prior approval of the Chief Legal Officer.

14.2 Any amendment shall enter into force after it has been approved and published on the Philips General Business Principles Internet site and communicated to the Business Customers.

14.3 Any request or claim of a Business Customer's Individual involving these Rules shall be judged against the version of these Rules that is in force at the time the request, complaint or claim is made.

14.4 The Chief Privacy Officer shall be responsible for informing the relevant government authorities of material changes to these Rules on a yearly basis and coordinating their responses. The Chief Privacy Officer shall inform the appropriate Senior Privacy Officers of the effect of these responses.

Article 15 – Transition Periods

General Transition Period

15.1 Except as otherwise indicated, Philips shall strive to comply with these Rules as soon as possible after the Effective Date. In any event all Processing of Personal Data that is subject to these Rules shall be conducted in compliance with the Rules within one year of the Effective Date.

Transition Period for New Group Companies

15.2 Any entity that becomes a Group Company after the Effective Date shall comply with the Rules within one year of becoming a Group Company.

Transition Period for Divested Entities

15.3 A Divested Entity will remain covered by these Rules after its divestment for such period as is required by Philips to disentangle the Processing of BCI Data relating to such Divested Entity.

Transition Period for IT Systems

15.4 Where implementation of these Rules requires updates or changes to information technology systems (including replacement of systems), the transition period shall be two years from the Effective Date or from the date an entity becomes a Group Company, or any longer period as is reasonably necessary to complete the update, change or replacement process.

Transition Period for Existing Agreements

15.5 Where there are existing agreements with Third Parties that are affected by these Rules, the provisions of the agreements will prevail until the agreements are renewed in the normal course of business.

ANNEX 1

Definitions

Adequate Country	ADEQUATE COUNTRY shall mean the EEA and those countries that the European Commission considers to provide an "adequate" level of data protection pursuant to Articles 25(6) and 31(2) EU Data Protection Directive.
Applicable Adequate Data Protection Law	APPLICABLE ADEQUATE DATA PROTECTION LAW shall mean the Data Protection Laws of an Adequate Country that are applicable to the Business Customer as the Data Controller of the BCI Data.
Applicable Data Processor Law	APPLICABLE DATA PROCESSOR LAW shall mean the Data Protection Laws that are applicable to Philips as the Data Processor of the BCI Data.
Business Customer	BUSINESS CUSTOMER shall mean the customer who has entered into a contract with Philips for the delivery of Philips Customer Services.
Business Customer's Individual	BUSINESS CUSTOMER'S INDIVIDUAL shall mean any individual whose Personal Data are Processed by Philips in its role as a Data Processor in the course of delivering Philips Customer Services to a Business Customer.
BCI Data	BCI DATA shall mean Personal Data of a Business Customer's Individual.
Business Customer Service Contract	BUSINESS CUSTOMER SERVICE CONTRACT shall mean the contract for delivery of Philips Customer Services entered into between a Philips Group Company and the Business Customer pursuant to Article 2.1.
Chief Legal Officer	CHIEF LEGAL OFFICER shall mean the chief legal officer of KPENV.
Chief Privacy Officer	CHIEF PRIVACY OFFICER shall mean the officer referred to in Article 8.1.

Country	COUNTRY shall mean each country in which a Group Company is established.
Country Privacy Officer	COUNTRY PRIVACY OFFICER shall mean the Senior Privacy Officer designated for a certain Country, in accordance with Article 8.3.
Customer Services	CUSTOMER SERVICES shall mean the services provided by Philips to Business Customers to support products and services of Philips or a Third Party. Such services may include the (remote) monitoring of patient or customer data or repair, maintenance, upgrade, replacement, inspection and calibration activities, the collection or provision of diagnostic or operational information, and related support activities aimed at facilitating continued and sustained use of products and services of Philips or a Third Party.
Data Controller	DATA CONTROLLER shall mean the entity or natural person which alone or jointly with others determines the purposes and means of the Processing of Personal Data.
Data Processor	DATA PROCESSOR shall mean the entity or natural person which Processes Personal Data on behalf of a Third Party Data Controller.
Data Protection Law	DATA PROTECTION LAW shall mean the laws of a country containing rules for the protection of individuals with regard to the Processing of Personal Data including security requirements for and the free movement of such Personal Data.
Data Security Breach	DATA SECURITY BREACH shall mean the unauthorized acquisition, access, use or disclosure of unencrypted BCI Data that compromises the security or privacy of such data to the extent the compromise poses a significant risk of financial, reputational, or other harm to the Business Customer's Individual. A Data Security Breach is deemed not to have occurred where there has been an unintentional acquisition, access or use of unencrypted BCI Data by an employee of Philips or the Business Customer or an individual acting under their respective authority, if (i) the acquisition, access, or use of BCI Data was made in good faith and within the course and scope of the employment or professional relationship of such employee or other individual; and (ii) the BCI Data are not further acquired, accessed, used or disclosed by any person.

Data Transfer Restriction	DATA TRANSFER RESTRICTION shall mean any restriction under the data protection laws of an Adequate Country regarding outbound transfers of Personal Data.
Divested Entity	DIVESTED ENTITY shall mean the divestment by Philips of a Group Company or business by means of: (a) a sale of shares as a result whereof the Group Company so divested no longer qualifies as a Group Company; and/or (b) a demerger, sale of assets, or any other manner or form.
EEA Countries	EEA COUNTRIES (European Economic Area Countries) shall mean all Member States of the European Union, Norway, Iceland, Liechtenstein and, for purposes of these Rules, Switzerland.
Effective Date	EFFECTIVE DATE shall mean the date on which these Rules become effective as set forth in Article 1.7.
Employee	EMPLOYEE shall mean an employee, job applicant or former employee of Philips.
EU Data Protection Directive	EU DATA PROTECTION DIRECTIVE shall mean the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
Function	FUNCTION shall mean a corporate department organized within Philips International (e.g. Corporate HRM, Corporate IT, Corporate Finance, Corporate Legal).
Function Privacy Officer	FUNCTION PRIVACY OFFICER shall mean the Senior Privacy Officer designated for a certain Function, in accordance with Article 8.3.
Group Company	GROUP COMPANY shall mean KPENV and any company or legal entity of which KPENV, directly or indirectly owns more than 50% of the issued share capital, has 50% or more of the voting power at general meetings of shareholders, has the power to appoint a majority of the directors, or otherwise directs the activities of such other legal entity; however, any such company or legal entity shall be deemed a Group Company only (i) as long as a liaison and/or relationship exists, and (ii) as long as it is covered by the Philips General Business Principles.

KPENV	KPENV shall mean Koninklijke Philips N.V., having its registered seat in Eindhoven, The Netherlands.
Mandatory Requirements	MANDATORY REQUIREMENTS shall mean mandatory requirements of Applicable Data Processor Law which do not go beyond what is necessary in a democratic society i.e. which constitute a necessary measure to safeguard national security defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the state or the protection of a Business Customer's Individual or the rights and freedoms of others.
Personal Data	PERSONAL DATA shall mean any information relating to an identified or identifiable individual.
Philips	PHILIPS shall mean KPENV and its Group Companies.
Philips Contracting Entity	PHILIPS CONTRACTING ENTITY shall mean the Philips Group Company that has entered into the Business Customer Service Contract.
Philips International	PHILIPS INTERNATIONAL shall mean Philips International B.V., having its registered seat in Eindhoven, The Netherlands.
Philips Privacy Council	PHILIPS PRIVACY COUNCIL shall mean the council referred to in Article 8.2.
Philips Sub-Processor	PHILIPS SUB-PROCESSOR shall mean any Group Company engaged by Philips as a Sub-Processor.
Privacy Officer	PRIVACY OFFICER shall mean the privacy officers appointed by the Senior Privacy Officers pursuant to Article 8.3.
Processing	PROCESSING shall mean any operation that is performed on BCI Data, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission or deletion of BCI Data.
Region	REGION shall mean a particular geographic area in which certain Countries are grouped.

Region Privacy Officer	REGION PRIVACY OFFICER shall mean the Senior Privacy Officer designated for a certain Region, in accordance with Article 8.3.
Relevant Data Protection Authority	RELEVANT DATA PROTECTION AUTHORITY shall mean any data protection authority that is competent to supervise the Business Customer as the Data Controller of the BCI Data.
Responsible Executive	RESPONSIBLE EXECUTIVE shall mean the lowest-level Philips business executive or the non-executive general manager of a Philips ORU (Organizational Reporting Unit) who has primary budgetary ownership of the relevant Processing.
Rules	RULES shall mean the Processor Privacy Rules for BCI Data.
Sector	SECTOR shall mean a top-level product division that is globally served by a specific Group Company, (e.g., Philips Healthcare, Philips Lighting, Philips Consumer Lifestyle).
Sector Privacy Officer	SECTOR PRIVACY OFFICER shall mean the Senior Privacy Officer designated for a certain Sector, in accordance with Article 8.3.
Senior Privacy Officers	SENIOR PRIVACY OFFICERS shall mean the appropriate Sector Privacy Officers, Function Privacy Officers, Country Privacy Officers and/or Region Privacy Officers.
Sensitive Data	SENSITIVE DATA shall mean Personal Data that reveal a Business Customer's Individual's racial or ethnic origin, political opinions or membership in political parties or similar organizations, religious or philosophical beliefs, membership in a professional or trade organization or union, physical or mental health including any opinion thereof, disabilities, genetic code, addictions, sex life, criminal offenses, criminal records, proceedings with regard to criminal or unlawful behavior, or social security numbers issued by the government.
Staff	STAFF shall mean all Employees and other persons who Process BCI Data as part of their respective duties or responsibilities using Philips information technology systems or working primarily from Philips premises.

Sub-Processor	SUB-PROCESSOR shall mean any Data Processor engaged to Process BCI Data as a sub-processor.
Third Party	THIRD PARTY shall mean any person or entity (e.g., an organization or government authority) outside Philips.
Third Party Sub-processor	THIRD PARTY SUB-PROCESSOR shall mean any Third Party engaged by Philips as a Sub-Processor.
Third Party Sub-processor Contract	THIRD PARTY SUB-PROCESSING CONTRACT shall mean the written contract entered into between the Philips Contracting Entity and the Third party Sub-processor pursuant to Article 7.1.

Interpretations

INTERPRETATION OF THESE RULES:

i. Unless the context requires otherwise, all references to a particular Article or Annex are references to that Article or Annex in or to this document, as they may be amended from time to time.
ii. Headings are included for convenience only and are not to be used in construing any provision of these Rules.
iii. If a word or phrase is defined, its other grammatical forms have a corresponding meaning.
iv. The female form shall include the male form.
v. The words “include,” “includes,” “including” and “e.g.”, and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa; and
vi. A reference to a document (including, without limitation, a reference to these Rules) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by these Rules or that other document.

ANNEX 2

Data Security

Security Policy Overview

IT systems and information are vital assets which are essential to Philips business. Philips has established an IT Security Framework, associated policies, and mandatory standards to protect the confidentiality, availability, and integrity of these assets.

The following provides an overview of those policies, procedures and processes that comprise the technical, physical and organizational measures employed by Philips to protect BCI Data from misuse or accidental, unlawful or unauthorized destruction, loss, alteration, disclosure, acquisition or access.

Philips IT Security Risk & Compliance Policy Framework
This document establishes the framework of IT security, risk, and compliance management policies and guidelines issued by Philips IT department. Each Philips business is responsible for integrating the controls based on appropriate risk assessments, and evolving industry standards.

Philips Information Security Policy - UDN 1596
This document describes objectives, responsibilities and mandatory rules for information security. This policy is derived from the Philips General Business Principles and is fully endorsed by the Philips Board of Management. This policy, along with the IT Security Controls document (see below), comprises the mandatory Philips Information Security Policies.

Philips IT Security Controls
The Philips IT Security Controls document is an extension of the Philips Information Security Policy (UDN 1596) and describes the control objectives, and key controls, including policies, processes, and procedures, organizational structures and software and hardware functions. This document is a statement of responsibilities of both Philips management and staff in order to establish and maintain an organization-wide secure IT environment. The following are examples of data security controls, further detailed in the Security Controls document:

- Data Classification
- Asset Accountability
- Encryption
- Training
- Physical Security Controls
- Security Risk Assessment
- System Planning and Acceptance
- Segregation of Duties
- Software Patching and Updates
- Backup and Restore
- Network Management Controls, including Audit Logging, Remote User Access, etc.
- Media Handling and Security, including Procedures for Secure Destruction of Data, etc.
- Exchange of Information and Software (between company systems)
- Access Controls
- Authentication
- Third-party Access Controls
- Mobile Computing

- Electronic Messaging
- Information Security Incident Management
- Business Continuity Management

Philips IT Security Standards, Guidelines and Baselines:
Additional documents set forth further direction for implementation of specific, required controls, including:

- User Account and Password Management
- Internal Firewall Policy
- IT Security Disk Encryption Policy
- IT Security Risk Assessment

Information Classification and Access Control

Philips regards information required for the pursuance of its business as a corporate asset, which must be protected against loss and infringements of its integrity and confidentiality. Each organizational unit is required by policy to assess risks to identified information assets and periodically check the level of security through security reviews. Information is classified into one of three categories, and each classification requires appropriate levels of security controls (e.g., encryption of data classified as secret or confidential). Philips Security Policy further requires that security measures for processing and storage of information be proportionate to classification level, and each user is to be uniquely identifiable, via personal user identification. Access controls exist to restrict access to systems and data to management authorized individuals for valid business purposes only. Philips Staff and Third Parties processing Philips information are accountable for the protection of that information and the applicable assets, per Philips Security Policies.

System Integrity and Availability

Each (Philips) organization is responsible for formal acceptance of the continuity of its business in the event of degradation or failure of the information infrastructure. Back-up copies of critical business information and software must be taken regularly and tested to ensure recovery. Contingency procedures must be tested at least annually, and workability of the contingency plan must be formally verified.

Activity Logging

Philips IT Security Controls require appropriate logging and monitoring to enable recording of IT security-relevant actions. IT Security features, service levels and management requirements of all network services must be identified and included in any network services agreement, whether these services are provided in-house or outsourced. Also, formal procedures are required for authorizing access to systems or applications, and all user access rights and privileges must be reviewed at regular intervals, at least quarterly.

Security Incidents

All employees, contractors, and third party users of information systems and services are required to note and report any observed or suspected security weaknesses in systems or services, through management channels, to Philips CSIRT (Computer Security Incident Response Team) for investigation and follow-up, as appropriate. IT Security incidents that involve personal data or that may have privacy implications must also be reported to the applicable Privacy Officer.

Physical Security

Philips IT Security Policy requires Philips management to identify those areas requiring specific level of physical security, and access to those areas is provided only to authorized persons for authorized purposes. Philips secured areas employ various physical security safeguards, including closed circuit television monitoring, use of security badges (identity controlled access) and security guards stationed at entry and exit points. Visitors may only be provided access where authorized and are to be supervised at all times.

Compliance

Philips has a standing Security Risk & Compliance organization (SRC) that regularly monitors the implemented security measures and implementation of new security requirements. Compliance with Philips IT Security Policies is accomplished through annual training, periodic reviews of local and organization-wide policies and procedures, and audits.