

Privacy Rules for Customer, Supplier and Business Partner Data

May 6, 2009

PHILIPS

Contact details

Philips Privacy Office

c/o Philips International BV

PO Box 218 (VO-1), 5600 MD Eindhoven, The Netherlands.

E-mail: Philips_Privacy_Office@philips.com

The most recent online version of the Privacy Rules for Customer, Supplier and Business Partner Data can be found on internet:

www.philips.com/shared/assets/Investor_relations/pdf/businessprinciples/PhilipsPrivacyRulesCSBData.pdf

Copyright

© Koninklijke Philips Electronics N.V., 2009

Amsterdam, The Netherlands

All rights reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner.

Version history

<i>Date</i>	<i>Updated sections</i>	<i>Version</i>
February 19, 2009	Initial version	1.0

Introduction

Philips General Business Principles express Philips commitment to strive to protect the Personal Data of Philips Customers, Suppliers and Business Partners. These Rules indicate how this commitment shall be implemented. For the privacy rules applicable to Employee personal data, refer to the *Privacy Rules for Employee Data*.

Article 1 – Scope, Applicability and Implementation

<i>Scope</i>	1.1 These Rules address the Processing of Personal Data (a) by or on behalf of Philips in its role as a Data Controller and (b) by Philips in its role as a Data Processor for Personal Data Processed in the course of delivering Philips Healthcare Customer Service. These Rules do not address the Processing of personal data of Philips Employees.
<i>Electronic and paper-based Processing</i>	1.2 These Rules apply to the Processing of Personal Data by electronic means and in systematically accessible paper-based filing systems.
<i>Sub-policies and notices</i>	1.3 Philips may supplement these Rules through sub-policies and notices that are consistent with these Rules.
<i>Compliance Responsibility</i>	1.4 These Rules are binding on Philips. The Responsible Executive shall be responsible for her business organization's compliance with these Rules. Philips Staff must comply with these Rules.
<i>Effective date</i>	1.5 These Rules enter into force as of May 6, 2009 (Effective Date). They are published on the General Business Principles Internet site.
<i>Rules supersede prior policies</i>	1.6 These Rules supersede all Philips privacy policies and notices that exist on the Effective Date to the extent they address the same issues or conflict with the provisions of these Rules.
<i>Implementation</i>	1.7 These Rules shall be implemented within Philips based on the timeframes specified in Article 22.
<i>Role of Philips International</i>	1.8 KPENV has tasked Philips International B.V. with the coordination and implementation of these Rules.
<i>Privacy Officer Advice</i>	1.9 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 – Purposes for Processing Personal Data

- Legitimate Business Purposes* **2.1** Personal Data shall be collected, used, transferred or otherwise Processed for one or more of the following purposes (**Business Purposes**):
- (i) **Legitimate purposes as appropriate to Philips business.** This addresses Processing necessary for activities such as marketing, sales, promotions, customer relations, account management, customer service, Philips Healthcare Customer Service, finance and accounting, research and development, purchasing, internal management and control, investor relations, external communications, government and legal affairs, alliances, ventures, mergers, acquisitions, divestitures, and intellectual property and standards management;
 - (ii) **Business process execution and internal management.** This addresses Processing necessary for activities such as managing company assets, conducting internal audits and investigations, and implementing business controls;
 - (iii) **Health, safety and security.** This addresses Processing necessary for activities such as those involving safety and health, the protection of Philips and Staff assets, and the authentication of Customer, Supplier or Business Partner status and access rights;
 - (iv) **Compliance with legal obligations.** This addresses Processing necessary for compliance with a legal obligation to which Philips is subject; or
 - (v) **Vital interests.** This addresses Processing necessary to protect a vital interest of an individual.
- Consent* **2.2** If none of the criteria listed in Article 2.1 applies, Philips shall obtain consent from the individual before Processing her Personal Data. In seeking consent, Philips must inform the individual of:
- (i) the purposes of the Processing for which consent is requested; and
 - (ii) any other relevant details to seek to ensure fair Processing.
- If the Processing is reasonably necessary to address a request of the individual (e.g., she subscribes to a service or seeks a benefit), the individual's consent is implied.
- Denial or withdrawal of consent* **2.3** The individual may deny or withdraw consent at any time.

Article 3 – Use for Other Purposes

Use of Personal Data for Secondary Purposes **3.1** Generally, Personal Data shall be used only for the purposes for which they were originally collected (**Original Purpose**). Personal Data may be Processed for a legitimate Business Purpose of Philips different from the Original Purpose (**Secondary Purpose**) only if the Original Purpose and Secondary Purpose are closely related.

If the purposes are not closely related or there is a potential for harm to the individual as a result of the use of her Personal Data for a closely-related Secondary Purpose, additional measures such as the following may be required:

- (i) limiting access to the Personal Data;
- (ii) implementing additional confidentiality and security controls;
- (iii) informing the individual about the Secondary Purpose;
- (iv) providing an opt-out opportunity; or
- (v) obtaining individual consent in accordance with Article 2.2.

Generally permitted uses of Personal Data for Secondary Purposes **3.2** It is generally permissible to use Personal Data for the following Secondary Purposes provided appropriate additional measures are taken in accordance with Article 3.1:

- (i) transferring the Personal Data to an Archive;
- (ii) conducting internal audits or investigations;
- (iii) implementing business controls;
- (iv) conducting statistical, historical or scientific research;
- (v) engaging in dispute resolution;
- (vi) using legal or business consulting services; or
- (vii) managing insurance issues.

Privacy Officer Advice **3.3** Before Processing Personal Data for a Secondary Purpose, Staff shall seek the advice of the appropriate Privacy Officer.

Article 4 – Purposes for Processing Sensitive Data

- Purposes for Processing Sensitive Data* **4.1** This Article sets forth specific rules for Processing Sensitive Data. Philips shall Process Sensitive Data only to the extent necessary to serve the applicable Business Purpose. Sensitive Data may be Processed under the following circumstances:
- (i) where the individual has explicitly consented to the Processing (“opt-in”);
 - (ii) where providing services (including health services) to the individual;
 - (iii) where Sensitive Data are Processed in connection with the purchase or use by an individual of a Philips product or service;
 - (iv) where the individual is voluntarily participating in a research project or product test;
 - (v) where Sensitive Data are Processed in the delivery of Philips Healthcare Customer Service;
 - (vi) as required by or allowed under applicable local law;
 - (vii) to establish, exercise or defend a legal claim;
 - (viii) to safeguard the security of Philips, a Group Company or its Employees (including Processing Sensitive Data in connection with site security e.g., photos, videos);
 - (ix) to safeguard the uninterrupted continuity of Philips business operations;
 - (x) to prevent, detect or prosecute (including cooperating with public authorities) suspected fraud, contract breaches, violations of law, or other breaches of the terms of access to Philips sites or assets;
 - (xi) to protect a vital interest of an individual, but only where it is impossible to obtain the individual’s consent first;
 - (xii) where the Sensitive Data have manifestly been made public by the individual; or
 - (xiii) where necessary to comply with an obligation of international public law.
- Prior Authorization of Chief Privacy Officer* **4.2** Where Sensitive Data are Processed based on a requirement of law other than the local law applicable to the Processing, or based on the consent of the individual, the Processing requires either (i) the prior approval of the appropriate Chief Privacy Officer or (ii) a privacy sub-policy governing the Processing.
- Use of Sensitive Data for Secondary Purposes* **4.3** Sensitive Data may be Processed for Secondary Purposes only in accordance with Article 3.

Article 5 – Quantity and Quality of Personal Data

<i>No excessive data</i>	5.1	Philips shall restrict the Processing of Personal Data to those data that are reasonably adequate for and relevant to the applicable Business Purpose. Philips shall take reasonable steps to securely delete or destroy Personal Data that are not required for the applicable Business Purpose.
<i>Retention period</i>	5.2	Philips generally shall retain Personal Data only: <ul style="list-style-type: none"> (i) for the period required to serve the applicable Business Purpose; (ii) to the extent reasonably necessary to comply with an applicable legal requirement; or (iii) as advisable in light of an applicable statute of limitations. Philips may specify (e.g., in a sub-policy, notice or records retention schedule) a time period for which certain categories of Personal Data will be kept.
<i>End of retention period</i>	5.3	Promptly after the applicable retention period has ended, the Responsible Executive shall direct that the Personal Data be: <ul style="list-style-type: none"> (i) securely deleted or destroyed; (ii) anonymized; or (iii) transferred to an Archive (unless this is prohibited by applicable local law or an applicable records retention schedule).
<i>Quality of Personal Data</i>	5.4	Personal Data should be accurate, complete and kept up-to-date to the extent reasonably necessary for the applicable Business Purpose.
<i>Informing Philips</i>	5.5	It is the responsibility of the individual to inform Philips if her Personal Data are inaccurate, incomplete or outdated and Philips shall rectify the data in accordance with Article 7.

Article 6 – Informing the individual

<i>Scope</i>	6.1	This Article addresses Philips obligations to inform individuals whose Personal Data are Processed by Philips in its role as a Data Controller.
<i>Information to the individual</i>	6.2	Philips shall inform the individual through a published privacy notice about: <ul style="list-style-type: none"> (i) the Business Purposes for which Personal Data are Processed; (ii) which Philips Group Company is responsible for the Processing; and (iii) other relevant information (e.g., the nature and categories of the Processed Personal Data, the categories of Third Parties to which the Personal Data are disclosed, if any, and how the individual can exercise her rights).

<i>Personal Data not obtained from the individual</i>	6.3	To the extent required by applicable law, where Personal Data have not been obtained directly from the individual, Philips shall provide the individual with information as required by Article 6.2 no later than the time the Personal Data are recorded in a Philips database.
<i>Exceptions</i>	6.4	The requirements of Article 6.3 may be set aside if: <ul style="list-style-type: none"> (i) it is impractical to inform the individual; or (ii) such provision of information would result in disproportionate cost.

Article 7 – Rights of individuals

<i>Scope</i>	7.1	This article addresses certain rights of individuals whose Personal Data are Processed by Philips in its role as a Data Controller.
<i>Rights of individuals</i>	7.2	Individuals have the right to request an overview of their Personal Data Processed by or on behalf of Philips. Where reasonably possible, the overview shall contain information regarding the source (if reasonably available), type, purpose and categories of recipients of the relevant Personal Data. <p>If the Personal Data are incorrect, incomplete or not Processed in compliance with applicable law or these Rules, the individual has the right to have her Personal Data rectified, deleted or blocked (as appropriate).</p> <p>The individual has the right to object to the Processing of her Personal Data on the basis of compelling grounds related to her particular situation.</p>
<i>Procedure</i>	7.3	To access, rectify, delete, or block Personal Data or to object to the Processing, the individual should send her request or objection to the contact person or contact point indicated in the relevant privacy notice. If no contact person or contact point is indicated, the individual may send her request or objection to Philips through the contact section of the relevant Philips website, or she may contact the appropriate Privacy Officer. <p>Prior to fulfilling the request of the individual, Philips may require the individual to:</p> <ul style="list-style-type: none"> (i) specify the type of Personal Data in question; (ii) specify, to the extent reasonably possible, the data system in which the Personal Data likely are stored; (iii) specify the circumstances in which Philips obtained the Personal Data; and (iv) show proof of her identity.

- Response period* **7.4** Within four weeks of Philips receiving the request or the objection, the Responsible Executive shall inform the individual in writing either (i) of Philips position with regard to the request or the objection and any action Philips has taken or will take in response or (ii) when she will be informed of Philips position.
- Complaint* **7.5** An individual may file a complaint in accordance with Article 17.1 if:
- (i) the response to the request or the objection is unsatisfactory to the individual (e.g., the request is denied); or
 - (ii) the individual has not received a response as required by Article 7.4.
- Denial of requests* **7.6** Philips may deny an individual's request or objection if:
- (i) the request or objection does not meet the requirements of Articles 7.2 and 7.3;
 - (ii) the request or objection is not sufficiently specific;
 - (iii) the identity of the relevant individual cannot be established by reasonable means;
 - (iv) the request or objection is made within an unreasonable time interval of a prior request or objection or otherwise constitutes an abuse of rights; or
 - (v) the Processing of the Personal Data is required by law.

Before denying a request or objection Staff shall seek the advice of the appropriate Chief Privacy Officer.

Article 8 – Security Requirements

- Data security* **8.1** Philips shall take appropriate commercially reasonable technical, physical and organizational measures to protect Personal Data from misuse or accidental, unlawful or unauthorized destruction, loss, alteration, disclosure, acquisition or access.
- Staff access* **8.2** Staff shall be provided access to Personal Data only to the extent necessary to serve the applicable Business Purpose and to perform their job.

Article 9 – Direct Marketing

- Consent for direct marketing* **9.1** To the extent required by applicable law, when Processing Personal Data for the purpose of making direct marketing communications, Philips will either:
- (i) obtain the prior affirmative consent (“opt-in”) of the targeted individual; or
 - (ii) offer the individual the opportunity to choose not to receive such communications (“opt-out”).

In every subsequent direct marketing communication that is made to the individual, the individual shall be offered the opportunity to opt-out of further marketing communication.

- Objection to marketing* **9.2** If the individual objects to receiving marketing communications from Philips, or withdraws her consent to receive such materials, Philips will take steps to refrain from sending further marketing materials as specifically requested by the individual. Philips will do so within the time period required by applicable law.

Article 10 – Automated Decision Making

- Automated decisions* **10.1** Automated tools may be used to make decisions about individuals but decisions may not be based solely on the results provided by the automated tool. This restriction does not apply if:
- (i) the use of automated tools is required or authorized by law; or
 - (ii) the decision is made by Philips for purposes of entering into or performing a contract provided that
 - (a) the underlying request leading to a decision by Philips was made by the individual (e.g., where automated tools are used to qualify contest entries or Process requests from Customers); or
 - (b) suitable measures are taken to safeguard the legitimate interests of the individual (e.g., the individual has been provided with an opportunity to express her point of view).

Article 11 – Transfer of Personal Data to Third Parties

- Transfer to Third Parties* **11.1** This Article sets forth requirements concerning the transfer of Personal Data from Philips to a Third Party. Note that a transfer of Personal Data includes situations in which
- (i) Philips discloses Personal Data to Third Parties (e.g., in the context of corporate due diligence); and
 - (ii) Philips provides remote access to Personal Data to a Third Party.

Third Party Data Controllers and Third Party Data Processors **11.2** There are two categories of Third Parties:

- (i) **Third Party Data Processors:** these are Third Parties that Process Personal Data solely on behalf of Philips and at its direction (e.g., Third Parties that Process Customer registration data on behalf of Philips); and
- (ii) **Third Party Data Controllers:** these are Third Parties that Process Personal Data and determine the purposes and means of the Processing (e.g., Philips business partners that provide their own goods or services to Customers).

Third Party Data Controller contracts **11.3** Third Party Data Controllers (other than public authorities) may Process Personal Data obtained in connection with their relationship with Philips only if they have a written contract with Philips. As appropriate, Philips shall seek to contractually protect the data privacy interests of impacted individuals. All such contracts shall be drafted in consultation with the appropriate Privacy Officer.

Business Contact Information may be transferred to a Third Party Data Controller without a contract if it is reasonably expected that such information will be used by the Third Party Data Controller to contact the individual for legitimate business purposes related to such individual's job responsibilities. However, Philips shall not transfer, sell, lease, or rent Business Contact Information in bulk to a Third Party Data Controller without consent except as permitted or required under applicable law and to the extent such transfer, sale, lease, or rent serves a legitimate Business Purpose (per Article 2.1).

*Third Party
Data Processor
contracts*

- 11.4** Third Party Data Processors may Process Personal Data in Philips role as a Data Controller only if the Third Party Data Processor has a written contract with Philips. The contract shall include provisions addressing the following:
- (i) the Third Party Data Processor shall Process Personal Data only in accordance with Philips instructions and for the purposes authorized by Philips;
 - (ii) the Third Party Data Processor shall keep the Personal Data confidential;
 - (iii) the Third Party Data Processor shall take appropriate technical, physical and organizational security measures to protect the Personal Data; and
 - (iv) the Third Party Data Processor shall not permit subcontractors to Process Personal Data in connection with its obligations to Philips without the prior written consent of Philips.

Furthermore, contracts with Third Party Data Processors shall include, as appropriate, provisions addressing the following:

- (v) Philips has the right to review the security measures taken by the Third Party Data Processor and the Third Party Data Processor shall submit its relevant data processing facilities to audits and inspections by Philips or any relevant government authority; and
- (vi) the Third Party Data Processor shall promptly inform Philips of any Information Security Incident involving Personal Data.

All such contracts shall be drafted in consultation with the appropriate Privacy Officer.

*Third Party Data
Processor to
Data Processor
contracts*

- 11.5** In the provision of Philips Healthcare Customer Service, Philips shall consult with the appropriate Privacy Officer and Legal Counsel in the preparation of contracts between Philips and Third Party Data Processors.

*Transfer of
Personal Data to
a Non-Adequate
Country*

11.6 This Article sets forth additional rules for the transfer of Personal Data to a Third Party located in a country that is not considered to provide an ‘adequate level of protection’ for Personal Data (**Non-Adequate Country**).

Personal Data may be transferred to a Third Party located in a Non-Adequate Country only if:

- (i) a contract has been concluded between Philips and the relevant Third Party that provides for safeguards at a similar level of protection as that provided by these Rules; the contract shall conform to any model contract requirement under applicable local law (if any);
- (ii) the Third Party has been certified under the United States Safe Harbor Program or any other similar program that is recognized as providing an ‘adequate’ level of data protection;
- (iii) the transfer is necessary for the performance of a contract with the Customer, Supplier or Business Partner or to take necessary steps at the request of the Customer, Supplier or Business Partner prior to entering into a contract;
- (iv) the transfer is necessary to protect a vital interest of the individual;
- (v) the transfer is necessary for the establishment, exercise or defense of a legal claim;
- (vi) the transfer is necessary to satisfy a pressing need to protect the public interests of a democratic society; or
- (vii) the transfer is required by any law to which the relevant Philips Group Company is subject.

To the extent permitted by law, items (vi) and (vii) above require the prior approval of the Royal Philips Chief Privacy Officer, who will consult the Chief Legal Officer prior to giving her approval. The Chief Legal Officer may delegate this responsibility to another executive within the Philips legal function.

*Transfers between
Non-Adequate
Countries*

11.7 This Article sets forth rules for transfers of Personal Data that were collected in connection with the activities of a Philips Group Company located in a Non-Adequate Country to a Third Party also located in a Non-Adequate Country. In addition to the grounds listed in Article 11.6, these transfers are permitted if they are:

- (i) necessary for compliance with a legal obligation to which the relevant Philips Group Company is subject;
- (ii) necessary to serve the public interest; or
- (iii) necessary to satisfy a Business Purpose of Philips.

Article 12 – Overriding Interests

- Overriding Interests* **12.1** Some of the obligations of Philips or rights of individuals under these Rules may be overridden if, under the specific circumstances at issue, a pressing legitimate need exists that outweighs the interest of the individual (**Overriding Interest**). An Overriding Interest exists if there is a need to:
- (i) protect the legitimate business interests of Philips including:
 - (a) the health, security or safety of individuals;
 - (b) Philips intellectual property rights, trade secrets or reputation;
 - (c) the continuity of Philips business operations;
 - (d) the preservation of confidentiality in a proposed sale, merger or acquisition of a business; or
 - (e) the involvement of trusted advisors or consultants for business, legal, tax, or insurance purposes.
 - (ii) prevent or investigate suspected or actual violations of (a) law (including cooperating with law enforcement), (b) contracts, or (c) or Philips policies; or
 - (iii) otherwise protect or defend the rights or freedoms of Philips, its Staff or other persons.
- Exceptions in the event of Overriding Interests* **12.2** If an Overriding Interest exists, one or more of the following obligations of Philips or rights of the individual may be set aside:
- (i) Article 3.1 (Use of Personal Data for Secondary Purposes);
 - (ii) Article 6.2 (Information to the individual);
 - (iii) Article 7.2 (Rights of individuals);
 - (iv) Article 8 (Data Security); and
 - (v) Articles 11.3, 11.4 and 11.6 (i) (Third Party Data Controller contracts, Third Party Data Processor contracts, Transfer of Personal Data to a Non-Adequate Country).
- Sensitive Data* **12.3** The requirements of Article 4.1 and 4.2 (Sensitive Data) may be set aside only for the Overriding Interests listed in this Article 12.1(i)(a), (c) and (e), (ii) and (iii).
- Consultation with Chief Privacy Officer* **12.4** Setting aside obligations of Philips or rights of individuals based on an Overriding Interest requires the prior consultation of the appropriate Chief Privacy Officer.
- Information to the individual* **12.5** Upon request of the individual, Philips shall inform the individual of the Overriding Interest that led to the setting aside of Philips obligations or the rights of the individual, unless the particular Overriding Interest sets aside the requirements of Articles 6.2 or 7.2, in which case the request shall be denied.

Article 13 – Supervision and compliance

- Royal Philips Chief Privacy Officer* **13.1** Philips International B.V. shall appoint a Royal Philips 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 Region Chief Privacy Officer, official investigations or inquiries into the Processing of Personal Data by a public authority.
- Philips Privacy Council* **13.2** The Royal Philips Chief Privacy Officer shall establish an advisory Privacy Council. The Privacy Council shall create and maintain a One Philips framework for:
- (i) the development, implementation and updating of local privacy sub-policies and procedures to include risk-based privacy impact assessments of databases, applications and business processes that Process Personal Data;
 - (ii) developing, implementing and updating relevant 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).

- Chief Privacy Officers* **13.3** Each Philips Sector shall designate a Sector Chief Privacy Officer and each Philips Region shall designate a Region Chief Privacy Officer. The Royal Philips Chief Privacy Officer shall act as the Chief Privacy Officer for Philips International B.V.. These Chief Privacy Officers may, in turn, establish a network of qualified Privacy Officers sufficient to direct compliance with these Rules within their respective organizations.
- The Chief Privacy Officers shall perform at least the following tasks:
- (i) regularly advise their respective executive teams and the Royal Philips Chief Privacy Officer on privacy risks and compliance issues;
 - (ii) maintain a registry, based on information supplied by the Responsible Executive, of all databases, applications, and business processes that Process Personal Data in their respective organization;
 - (iii) implement the privacy compliance framework as required by the Royal Philips Chief Privacy Officer;
 - (iv) be available for requests for privacy approvals 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 Royal Philips Chief Privacy Officer, other Chief Privacy Officers, the Privacy Officers, and the General Business Principles Compliance Officers.
- Responsible Executive* **13.4** The Responsible Executive shall perform at least the following tasks:
- (i) provide information necessary to support the maintenance of the registry of all databases, applications, and business processes that Process Personal Data in her organization;
 - (ii) ensure that Privacy Impact Assessments are performed and signed off on all systems and processes that Process Personal Data;
 - (iii) inform the individual in writing (as required by Article 7.4);
 - (iv) direct that Personal Data are securely deleted or destroyed, anonymized or transferred to an Archive promptly after the end of the retention period (as required by Article 5.3);
 - (v) determine how to comply with the Rules when there is a conflict with applicable law (as required by Article 20.2); and
 - (vi) inform the appropriate Chief Privacy Officers of any new legal requirement that may interfere with Philips ability to comply with these Rules (as required by Article 20.3).
- Default Privacy Officer* **13.5** If no Chief Privacy Officer has been designated in a Sector or Region, the designated compliance officer for the Philips General Business Principles for the relevant Group Company is responsible for supervising compliance with these Rules.

Privacy Officers with statutory position **13.6** Where a Privacy Officer holds her position pursuant to law, she shall carry out her job responsibilities to the extent they do not conflict with her statutory position.

Article 14 – Policies and procedures

Policies and procedures **14.1** Philips shall develop and implement policies and procedures to comply with these Rules.

Article 15 – Training

Staff training **15.1** 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 Personal Data.

Article 16 – Monitoring compliance

Audits **16.1** Philips Internal Audit shall audit business processes and procedures that involve the Processing of Personal 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 a Chief Privacy Officer. The Royal Philips 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 Royal Philips Chief Privacy Officer and the appropriate Chief Privacy Officers shall be informed of the results of the audits.

Annual Report **16.2** The Royal Philips Chief Privacy Officer shall produce an annual Customer, Supplier and Business Partner privacy report for the Chief Legal Officer on compliance with these Rules and other relevant issues.

Each Chief Privacy Officer shall provide information relevant to the annual privacy report to the Royal Philips Chief Privacy Officer.

Article 17 – Complaint procedure

- Complaint to Privacy Officer* **17.1** Individuals may file a complaint regarding compliance with these Rules:
- (i) in accordance with the complaint procedure set forth in the relevant privacy policy or contract; or
 - (ii) with the appropriate Privacy Officer who, in turn, shall
 - (a) notify the appropriate Chief Privacy Officers who shall initiate an investigation;
 - (b) when necessary, advise the organization on the appropriate measures for compliance; and
 - (c) when measures are undertaken, monitor the steps designed to achieve compliance until all compliance measures are completed.

The appropriate Chief Privacy Officers may consult with any government authority having jurisdiction over a particular matter about the measures to be taken.

- Reply to the individual* **17.2** Within four weeks of Philips receiving a complaint, the appropriate Chief Privacy Officer shall inform the individual in writing either:
- (i) of Philips position with regard to the complaint and any action Philips has taken or will take in response; or
 - (ii) when she will be informed of Philips position.

The appropriate Chief Privacy Officer shall send a copy of the complaint and any written reply to the Royal Philips Chief Privacy Officer.

- Complaint to Royal Philips Chief Privacy Officer* **17.3** An individual may file a complaint with the Royal Philips Chief Privacy Officer if:
- (i) the resolution of the complaint by the appropriate Chief Privacy Officer is unsatisfactory to the individual (e.g., the complaint is rejected);
 - (ii) the individual has not received a response as required by Article 17.2; or
 - (iii) the time period provided to the individual pursuant to Article 17.2 is, in light of the relevant circumstances, unreasonably long and the individual has objected but has not been provided with a shorter, more reasonable time period in which she will receive a response.

- Appeals to responses from the Royal Philips Chief Privacy Officer* **17.4** The procedure described in Articles 17.1 through 17.3 shall apply to complaints filed with the Royal Philips Chief Privacy Officer. Appeals to responses from the Royal Philips Chief Privacy Officer should be directed to the Royal Philips Chief Legal Officer if at least one of the conditions of 17.3(i), 17.3(ii), or 17.3(iii) is satisfied.

Article 18 – Legal issues

- | | |
|---|---|
| <i>Local law and jurisdiction</i> | 18.1 Any Processing by Philips of Personal Data shall be governed by applicable local law. Individuals keep any rights and remedies they may have under applicable local law. Local public authorities having jurisdiction over the relevant matters maintain their authority. |
| <i>Supplemental protection provided by Rules</i> | 18.2 These Rules shall apply only where they provide supplemental protection for Personal Data. Where applicable local law provides more protection than these Rules, local law shall apply. Where these Rules provide more protection than applicable local law or provide additional safeguards, rights or remedies for individuals, these Rules shall apply. |
| <i>Lead Authority for supervision of Rules</i> | 18.3 Compliance with these Rules shall be exclusively supervised by the Dutch Data Protection Authority (College Bescherming Persoonsgegevens) in The Netherlands, which is also exclusively authorized to advise Philips International B.V. on the application of these Rules at all times. The Dutch Data Protection Authority shall have investigative powers based on the Dutch Data Protection Act (Wet bescherming persoonsgegevens). To the extent the Dutch Data Protection Authority has discretionary powers related to enforcement of the Dutch Data Protection Act, it shall have similar discretionary powers for enforcement of these Rules. |
| <i>Exclusive jurisdiction under Rules</i> | 18.4 Any complaints or claims of an individual concerning any supplemental right the individual may have under these Rules shall be directed to Philips International B.V. only and shall be brought before the Dutch Data Protection Authority in The Netherlands or the competent court in Amsterdam, The Netherlands. The Dutch Data Protection Authority and courts in Amsterdam, The Netherlands have exclusive jurisdiction over any supplemental rights provided by these Rules. Complaints and claims shall be admissible only if the individual has first followed the complaint procedure set forth in Article 17 of these Rules. |
| <i>Additional Forum under Rules</i> | 18.5 If a Group Company established in one of the EEA countries (the Exporting Group Company) transfers Personal Data to a Group Company located in a Non-Adequate Country (the Importing Group Company) and the Importing Group Company violates these Rules, the individual may enforce these Rules against the Exporting Group Company before the courts in the country in which the Exporting Group Company is established. The individual shall have rights and remedies against the Exporting Group Company as if the violation had taken place by the Exporting Group Company instead of the Importing Group Company. |
| <i>Rules enforceable against Philips International only</i> | 18.6 Any additional safeguards, rights or remedies granted to individuals under these Rules are granted by and enforceable in the Netherlands against Philips International B.V. only. |

Available remedies and limitation of damages **18.7** Under these Rules, individuals shall only be entitled to remedies available to data subjects under the Dutch Data Protection Act, the Dutch Civil Rules and the Dutch Rules on Civil Procedure. However, Philips International B.V. 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 an individual resulting from a violation of these Rules.

Mutual assistance and redress **18.8** All Group Companies shall cooperate and assist each other to the extent reasonably possible to handle issues including:

- (i) a request, complaint or claim made by an individual; or
- (ii) an investigation or inquiry by a public authority.

The Philips organization (e.g., Royal Philips, a Group Company) receiving the individual's request, complaint or claim is responsible for handling any communication with the individual regarding her request, complaint or claim except where circumstances dictate otherwise and as mutually agreed among Chief Privacy Officers relevant to the specific issue.

The Group Company that is responsible for the Processing to which the request, complaint or claim relates, shall bear all costs involved and reimburse Philips International B.V.

Article 19 – Sanctions for non-compliance

Non-compliance **19.1** Non-compliance of Philips employees with these Rules may result in disciplinary action up to and including termination of employment.

Article 20 – Conflicts between the Rules and applicable local law

Conflict of law when transferring Personal Data **20.1** Where a legal requirement to transfer Personal Data conflicts with the laws of the Member States of the EEA or other countries with legal requirements regarding cross-border data transfer, any relevant Personal Data transfer requires the prior approval of the Chief Legal Officer. The Chief Legal Officer shall seek the advice of the appropriate Chief Privacy Officers. The Chief Privacy Officers may seek the advice of the Dutch Data Protection Authority or another competent public authority.

Conflict between Rules and law **20.2** In all other cases, where there is a conflict between applicable local law and the Rules, the relevant Responsible Executive shall consult with the appropriate Chief 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 **20.3** The relevant Responsible Executive, in consultation with her legal department, shall promptly inform the appropriate Chief Privacy Officers of any new legal requirement that may interfere with Philips ability to comply with these Rules.

Article 21 – Changes to the Rules

- 21.1** Any changes to these Rules require the prior approval of the Chief Legal Officer.
- 21.2** Any amendment shall enter into force after it has been approved and published on the Philips General Business Principles Internet site.
- 21.3** Any request, complaint or claim of an 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.
- 21.4** The Royal Philips Chief Privacy Officer shall be responsible for informing the relevant government authorities of any changes to these Rules and coordinating their responses. The Royal Philips Chief Privacy Officer shall inform the appropriate Philips Chief Privacy Officers of the effect of these responses.

Article 22 – Transition Periods

- General Transition Period* **22.1** Except as indicated below, there shall be a two-year transition period for compliance with these Rules. Accordingly, except as otherwise indicated, within two years of the Effective Date, all Processing of Personal Data that is subject to these Rules shall be conducted in compliance with the Rules. During any transition period, Philips shall strive to comply with the Rules.
- Transition Period for New Group Companies* **22.2** Any entity that becomes a Group Company after the Effective Date shall comply with the Rules within two years of becoming a Group Company.
- Transition Period for IT Systems* **22.3** Where implementation of these Rules requires updates or changes to information technology systems (including replacement of systems), the transition period shall be four 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* **22.4** 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.

Transition Period for Local-for-Local Systems **22.5** Processing of Customer, Supplier or Business Partner Personal Data that were collected in connection with activities of a Philips Group Company located in a Non-Adequate Country shall be brought into compliance with these Rules within five years of the Effective Date.

ANNEX 1

Definitions

<i>Archive</i>	ARCHIVE shall mean a collection of Personal Data that are no longer necessary to achieve the purposes for which the Personal Data originally were collected or that are no longer used for general business activities, but are used only for historical, scientific or statistical purposes, dispute resolution, investigations or general archiving purposes. An archive includes any data set that is subject to appropriately enhanced security and has restricted access (e.g., only by the system administrator and responsible executive).
<i>Business Contact Information</i>	BUSINESS CONTACT INFORMATION shall mean personal information typically found on a business card that is used by an individual in the conduct of her employment.
<i>Business Partner</i>	BUSINESS PARTNER shall mean any (a) individual or (b) individual associated with an entity, other than a Customer or Supplier, which has a business relationship or strategic alliance with Philips (such as a joint marketing partner, joint venture or joint development partner).
<i>Business Purpose</i>	BUSINESS PURPOSE shall mean a purpose for Processing Personal Data as specified in Article 2 or 3 or for Processing Sensitive Data as specified in Article 4.
<i>Chief Legal Officer</i>	CHIEF LEGAL OFFICER shall mean the chief legal officer of KPENV.
<i>Chief Privacy Officers</i>	CHIEF PRIVACY OFFICERS shall mean the Sector Chief Privacy Officers and the Region (Area) Chief Privacy Officers.
<i>Customer</i>	CUSTOMER shall mean any (a) individual or (b) individual associated with an entity, which purchases or may purchase a Philips product or service.
<i>Data Controller</i>	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.
<i>Data Processor</i>	DATA PROCESSOR shall mean the entity or natural person which Processes Personal Data on behalf of the Data Controller.
<i>EEA</i>	EEA or EUROPEAN ECONOMIC AREA shall mean all Member States of the European Union, plus Norway, Iceland and Liechtenstein.
<i>Effective Date</i>	EFFECTIVE DATE shall mean the date on which these Rules become effective as set forth in Article 1.5.
<i>Employee</i>	EMPLOYEE shall mean an employee, job applicant or former employee of Philips.

<i>EU Data Protection Directive</i>	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.
<i>Exporting Group Company</i>	EXPORTING GROUP COMPANY shall mean the Group Company located within the EEA that transfers Personal Data to a Group Company located in a Non-Adequate Country.
<i>Group Company</i>	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 as long as a liaison and/or relationship exists, and that is covered by the Philips General Business Principles (unless excepted by the General Secretary).
<i>Importing Group Company</i>	IMPORTING GROUP COMPANY shall mean a Group Company located within a Non-Adequate Country that receives Personal Data from an Exporting Group Company.
<i>Information Security Incident</i>	INFORMATION SECURITY INCIDENT shall mean any actual or suspected theft, or unauthorized Processing, loss, use, disclosure, or acquisition of, or access to, any data.
<i>KPENV</i>	KPENV shall mean Koninklijke Philips Electronics N.V., having its registered seat in Eindhoven, The Netherlands.
<i>Non-Adequate Country</i>	NON-ADEQUATE COUNTRY shall mean a country that under applicable local law (such as Article 25 of the EU Data Protection Directive) is deemed not to provide an “adequate” level of data protection.
<i>Original Purpose</i>	ORIGINAL PURPOSE shall mean the purpose for which Personal Data was originally collected.
<i>Overriding Interest</i>	OVERRIDING INTEREST shall mean a pressing legitimate need that under specific circumstances outweighs the interest of the individual.
<i>Personal Data</i>	PERSONAL DATA shall mean any information relating to an identified or identifiable individual where the individual is associated with a Philips Customer, Supplier or Business Partner.
<i>Philips</i>	PHILIPS shall mean KPENV and its Group Companies.
<i>Philips Healthcare</i>	PHILIPS HEALTHCARE shall mean a business Sector of KPENV.

<i>Philips Healthcare Customer Service</i>	PHILIPS HEALTHCARE CUSTOMER SERVICE shall mean the services provided by Philips Healthcare to Philips Healthcare Customers to support Philips Healthcare products, including: 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 Philips Healthcare products.
<i>Philips International</i>	PHILIPS INTERNATIONAL shall mean Philips International B.V., having its registered seat in Eindhoven, The Netherlands.
<i>Philips Privacy Council</i>	PHILIPS PRIVACY COUNCIL shall mean the council referred to in Article 13.2.
<i>Privacy Officer</i>	PRIVACY OFFICER shall mean the privacy officers appointed by the Chief Privacy Officers pursuant to Article 13.3.
<i>Processing</i>	PROCESSING shall mean any operation that is performed on Personal 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 Personal Data.
<i>Region</i>	REGION shall mean a particular geographic area that is served by a specific Group Company.
<i>Responsible Executive</i>	RESPONSIBLE EXECUTIVE shall mean the lowest-grade Philips business executive who has primary budgetary ownership over the relevant Processing.
<i>Region Chief Privacy Officer</i>	REGION CHIEF PRIVACY OFFICER shall mean the officer referred to in Article 13.3.
<i>Royal Philips Chief Privacy Officer</i>	ROYAL PHILIPS CHIEF PRIVACY OFFICER shall mean the officer referred to in Article 13.1.
<i>Rules</i>	RULES shall mean the Privacy Rules for Customer, Supplier and Business Partner Data.
<i>Secondary Purpose</i>	SECONDARY PURPOSE shall mean any purpose other than the Original Purpose for which Personal Data is further Processed.
<i>Sector</i>	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).
<i>Sector Chief Privacy Officer</i>	SECTOR CHIEF PRIVACY OFFICER shall mean the officer referred to in Article 13.3.

<i>Sensitive Data</i>	SENSITIVE DATA shall mean Personal Data that reveal an 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.
<i>Staff</i>	STAFF shall mean all Employees and other persons who Process Personal Data as part of their respective duties or responsibilities using Philips information technology systems or working primarily from Philips premises.
<i>Supplier</i>	SUPPLIER shall mean any (a) individual or (b) individual associated with an entity, which provides goods or services to Philips (such as an agent, consultant or vendor).
<i>Third Party</i>	THIRD PARTY shall mean any person or entity (e.g., an organizations or government authority) outside Philips.
<i>Third Party Data Controller</i>	THIRD PARTY DATA CONTROLLER shall mean a Third Party that Processes Personal Data and determines the purposes and means of the Processing.
<i>Third Party Data Processor</i>	THIRD PARTY DATA PROCESSOR shall mean a Third Party that Processes Personal Data on behalf of Philips that is not under the direct authority of Philips.

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.

