

Data Protection Policy

APR Group of Companies

Version 1.0

October 2018

TABLE OF CONTENTS

1 – INTRODUCTION	3
1.1 – Objective and Definitions	3
1.2 – Scope	5
1.3 – Principles for Processing Personal Data	5
1.4 – Highly Sensitive Data	8
1.5 – Personal Data APR Group collects	9
1.6 – How APR collects Personal Data	9
2 – EMPLOYEE DATA	11
2.1 – Data processing for employment relationship	11
2.2 – Data processing pursuant to legal authorization	13
2.3 – Consent to Data processing	13
2.4 – Data processing for legitimate interest	13
2.5 – Automated decision	14
2.6 – Telecommunication and Internet	15
3 – THIRD PARTY DATA.....	16
3.1 – Third Party Data.....	16
3.2 – Social Media and Internet.....	17
3.3 – Consent to Process	18
4 – DATA TRANSMISSION.....	19
4.1 – Transmission of the Data	19
4.2 – Processing by Third Parties	19
5 – DATA SUBJECT RIGHTS.....	21
6 – CONFIDENTIALITY.....	22
7 – POLICY COMPLIANCE.....	23
7.1 – Responsibilities and Sanctions.....	24
7.2 – Contacts	24

1. INTRODUCTION

1.1 Objective and Definitions

Objective.

As part of its social responsibility, APR Applied Pharma Research s.a. ("APR"), together with all its subsidiary companies belonging to the group (the "APR Group"), is committed to international compliance with data protection laws and, in particular, with the General Data Protection Regulation N. 679/2016 of April 27th, 2016 (the "GDPR"). This Data Protection Policy (the "Policy") is based on globally accepted, basic principles on data protection and applies to all the companies of the APR Group.

The main purpose of this Policy is to ensure that all companies belonging to the APR Group are in full compliance with regulations on the protection of Personal Data (as defined), worldwide and to assure an adequate level of data protection as prescribed by the GDPR and the national applicable laws for the cross – border data transmission, including in the countries that do not have data protection laws.

APR must ensure that Personal Data are carefully processed and used appropriately for the purpose of their collection. In adopting the present Policy on the protection of Personal Data, APR is pursuing three objectives:

- Establishing a uniform standard to be applied by all the companies belonging to the APR Group in processing Personal Data;
- Providing preventive safeguards against the infringement of personality and privacy rights through the inappropriate processing of Personal Data;
- Providing an adequate level of protection of Personal Data as required by the laws.

Definitions.

For the purpose of this Policy, the following definitions shall apply:

Data Subject: the natural or legal person to which the Personal Data refer.

Data Processor: any natural or legal person, public administration, body, association or other organization or entity that processes the Personal Data on the Data Controller's behalf.

Data Controller: any natural or legal person, public administration, body, association or other organization or entity that is responsible for determining the purposes and methods of the processing of Personal Data.

Highly Sensitive Data: any data related to racial or ethnic origin, political opinions, religious or philosophical beliefs, union membership, sexual life, physical or mental health, social security measures, administrative or criminal proceedings and sanctions of the Data Subject. This definition shall automatically include any data that shall be considered highly sensitive under the applicable national laws.

Individuals: any current, prospective and former clients, employees, consultants, customers, patients, healthcare professionals, subjects for clinical trials or other programs related to the research, development and commercialization of drugs and other healthcare products, healthcare providers or persons that refer, recommend or may influence the purchase or prescribing of APR Group's products, visitors and guests of APR Group Sites and, in general, persons that may authorize the collection of their Personal Data.

Personal Data: any information relating to an identified or identifiable natural or legal person.

Processing: any operations or set of operations on Personal Data carried out with or without electronic instruments. Such operations can be including but not limited to: collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, interrogation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Site: any APR Group website.

1.2 Scope

Based on this Policy, the APR Group declares that compliance with data protection principles in the processing of Personal Data (e.g. data on patients, health professionals, customers, suppliers, patients or care givers' associations, employees, etc.) is a corporate objective.

As a healthcare group, the APR Group treats personal medical data (e.g. data collected in connection with clinical trials or registries, etc.) with special care. Where Personal Data are processed by third parties on behalf of the APR Group's, appropriate measures shall be taken to ensure the full compliance of such third parties with the principles set forth in this Policy.

National legislations providing more comprehensive safeguards of Personal Data must be followed and implemented in all specific instances where such legislation applies.

This Policy applies to all APR Group's companies, subsidiaries and employees of such companies. All APR Group employees involved in Processing data are responsible for implementing and enforcing compliance with this Policy. This Policy applies to Personal Data Processed by the APR Group in the course of business, including on its Sites. Any Processing of Personal Data on behalf of the APR Group has to be conducted in full adherence to this Policy.

The companies of the APR Group are not allowed to adopt policies related to data Processing that are not in full compliance with this Policy, nor may they amend this Policy without a written authorization of APR's CEO. Each subsidiary company belonging to the APR Group shall have the right to introduce and implement additional, locally applicable and specific Privacy Policy in order to additionally safeguard Processing and protection of Personal Data whenever necessary or advisable in consideration of the specific business activity of such subsidiary. Any local Privacy Policy shall have to be approved by the Board of Directors of the subsidiary and shall have to be in full compliance with the present Privacy Policy.

This Policy comprises the internationally accepted data privacy principles without replacing the existing national laws. In the event of conflict between this Privacy Policy and any relevant national law, the latter shall prevail

on this Privacy Policy.

In the event of doubt in relation to the application of this Privacy Policy or a possible conflict between this Privacy Policy and any applicable law, the relevant APR Group company (or any of its employees that faces such doubt) must contact the Corporate Legal office of APR at the following address: privacy@apr.ch.

Considering that APR is a Swiss Company conducting business in many European countries directly through its subsidiaries or indirectly through commercial partners, in order to secure compliance of this Privacy Policy with the European GDPR, the Board of Directors of APR has resolved as follows:

- to have the parent company APR appointed as Data Controller for Data Processing at corporate level, and
- to have its subsidiary company APR Applied Pharma Research Italy s.r.l. (“APR Italy”) appointed as Data Controller for Data Processing within the European Union.

APR and APR Italy have respectively appointed the corporate Head of Legal Department as Data Protection Officer at both corporate and subsidiary level.

The latest version of this Policy can be accessed on the main APR corporate website: www.apr.ch.

The present version of this Policy is identified as follows:

Abbreviated Name: **Privacy Policy**

Identification Number: **Version 1.0**

Board Approval Date: **October 31st, 2018.**

Any future amendment, modification, addition or deletion shall be identified with a new Identification Number and shall require a new Board approval.

1.3 Principles for processing Personal Data

The following principles in processing Personal Data shall apply:

a) **Fairness and lawfulness.** When processing Personal Data, the individual rights of the Data Subjects must be protected. Personal Data must be collected and processed in a legal and fair manner.

b) **Restriction to a specific purpose.** Personal Data are obtained and processed only where this is strictly necessary for specified, fair and legitimate purposes. Personal Data can be processed only for the purpose that was defined before the data was collected. Subsequent changes to the purpose are only possible to a limited extent and require substantiation.

c) **Transparency.** The Data Subject must be informed of how his/her data is being handled. In general, Personal Data must be collected directly from the individual concerned. When the data is collected, the Data Subject must either be aware of, or informed of:

- » The identity of the Data Controller
- » The purpose of data Processing
- » Third parties or categories of third parties to whom the data might be transmitted.

d) **Data reduction and data economy.** Personal Data cannot be collected without a specific purpose. Before processing Personal Data, it must determine whether and to what extent the processing of Personal Data is necessary in order to achieve the purpose for which it is undertaken. Where the purpose allows and where the expense involved is in proportion with the goal being pursued, anonymized or statistical data must be used. Personal Data may not be collected in advance and stored for potential future purposes unless required or permitted by national law.

e) **Deletion.** Personal Data cannot be maintained after accomplishment of the purpose in relation to such data were collected. They cannot be maintained after the expiration of the process-related period and must be deleted accordingly.

f) **Accuracy; up-to-dateness of data.** All Personal Data must be

kept both accurate and up to date. Errors must be corrected effectively and promptly. Personal Data on file must be correct, complete, and – if necessary – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented or updated.

g) **Confidentiality and data security.** Personal Data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction.

h) **Collection Limitation.** The collection of Personal Data must be adequate, lawful, relevant and not excessive. No Personal Data may be collected without consent and if not immediately necessary for the purpose as originally defined. The collection of Personal Data and the purpose of its processing must be evident to the Data Subject.

1.4 Highly Sensitive Data

Highly Sensitive Data may be processed only when such processing is required by law (for example in order to start an employment relationship) or is allowed by law and their collection and processing is not avoidable and related to specific purpose.

In such events, Data Subjects has to be previously informed about the nature of the processing, the reason of the processing and his consent to such processing has to be obtained. In addition, particular measures must be implemented to ensure the maximum protection under any circumstance of the data collected.

1.5 Personal Data

For its business activities, the APR Group may collect Personal Data that may be deemed personal information, such as title, name, address, age, birth date, phone number, email address, user name, government identification (e.g., driver's license, passport), photo or image, Internet Protocol address, and credit card and other financial information related to payments for services or goods, as applicable.

The APR Group may also collect other Personal Data such as demographic information an Individual choose to provide (e.g., business or company information, professional experiences, educational background, nationality, ethnic origin, gender, interests, preferences and favourites) and answers to a security question and password.

In addition, if an Individual participates in certain programs or services, the APR Group may collect, on voluntary basis, Personal Data regarding medications, medical history and other healthcare-related information, including, Highly Sensitive Information (e.g. health information, diagnosis and treatment).

1.6 How APR collects Personal Data

The APR Group may, on voluntary basis, collect Personal Data through various channels, including its websites (the "Sites"), in surveys, during business or marketing events, conferences and conventions or when delivering programs and services to third parties.

In particular, the APR Group may collect Personal Data for the following reasons:

- When an Individual uses the Sites, the APR Group may provide opportunities to sign up to receive specific information or services and may ask for contact information (e.g. name, home address, home phone number or

personal email address).

- When an Individual navigates the Sites, certain passive information may also be collected, including Internet Protocol addresses, cookies, navigational data, the name of the domain and host from which it accesses the Internet, the browser software it uses and its operating system, the date and time of access the Sites, the Internet address of the website from which the Individual linked directly to the Sites. This type of information is used for the purposes of gathering data to provide improved administration of the Sites, and to improve the quality of the experience when interacting with the Sites. In addition, each Site provides detailed information in relation to its cookie policies.
- The APR Group is also obligated to collect certain Personal Data to comply with regulatory requirements, including information relating to adverse effects that Individuals experienced using APR Group products.
- The APR Group does not collect Personal Data from Third-Party sources and, if it happens, such data are provided to the APR Group in anonymous form from a source authorized for the Processing and transfer such data.
- The APR Group may perform research (online and offline) via surveys. The APR Group may engage third party-service providers to conduct such surveys on its behalf. All survey responses are voluntary, and the information collected shall be used for research and reporting purposes to improve services and products offered by the APR Group. The APR Group may also share anonymous individual and aggregate data for research and analysis purposes.

2. EMPLOYEE DATA

2.1 Data Processing for employment relationship

Personal Data can be processed in any event this is necessary to start, continue or terminate an employment relationship.

When initiating an employment relationship, the applicants' Personal Data can be processed. If the candidate is rejected, his/her data must be deleted in observance of the required retention period, unless the applicant has agreed to remain on file for a future selection process. Consent is also needed to use the data for further application processes or before sharing the application with other companies belonging to the APR Group.

For the existing employment relationship, the Personal Data must be processed only within the scope of the employment relationship and in accordance with the applicable laws. Particular restriction in relation to the processing of the data imposed by local applicable regulation, such as, but not limited to, collective regulations with employee representatives or the legitimate interest of the company, must be respected. In any case, Personal Data may be processed only upon voluntary authorization and, in the event such authorization has not been obtained when the employment relationship started, it has to be obtained in writing or electronically.

High Sensitive Data may be necessary to start, continue or terminate an employment relationship with an APR Group company (for example a declaration that certifies the absence of criminal convictions). In such events, such data may be collected and processed only in accordance with the applicable laws and within the limits necessary for the starting, maintenance and termination of the employment relationship.

Personal Data collected for employment purposes, may also be transmitted to third parties (and processed by those parties) for the exclusive purpose to start, continue or terminate the employment relationship. In particular, Personal Data of employees may be communicated to banks (for salary payments), external accountants, tax and fiscal authorities, external

auditors. In such case, communication must adhere to the principles of this Policy and to the applicable privacy law.

Beside this, the APR Group may hold, use and process Personal Data of its employees for a variety of business purposes including:

- a. workflow management, assigning, managing and administering projects, including clinical trials or other programs related to the research, development and commercialization of drugs and other healthcare products;
- b. human resources administration and communication;
- c. payroll and the provision of benefits;
- d. compensation, including bonuses and long-term incentive administration, stock plan administration, compensation analysis, including monitoring overtime and compliance with labor laws, and company recognition programs;
- e. job grading activities;
- f. performance and employee development management;
- g. organizational development and succession planning;
- h. benefits and personnel administration;
- i. absence management;
- j. helpdesk and IT support services;
- k. regulatory compliance;
- l. internal and/or external or governmental compliance investigations;
- m. internal or external audits;
- n. litigation evaluation, prosecution and defense;
- o. diversity and inclusion initiatives;
- p. restructuring and relocation;
- q. emergency contacts and services;
- r. safety;
- s. compliance with statutory requirements;
- t. Processing of employee expenses and travel charges; and
- u. acquisitions, divestitures and integrations

2.2 Data Processing pursuant to legal authorization

The Processing of employees' Personal Data is also permitted if national legislation requests, requires or authorizes this. The type and extent of data processing must be necessary for the legally authorized data Processing activity, and must comply with the relevant statutory provisions. If there is some legal flexibility, the interests of the employee that merit protection must be taken into consideration.

2.3 Consent to Data Processing

Employee data can be Processed upon consent of the Data Subject.

Declarations of consent must be submitted voluntarily. Involuntary consent is void. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In certain circumstances, consent may be given verbally, in which case it must be properly documented.

Before giving consent, the data subject must be informed in accordance with this Policy.

2.4 Data Processing for legitimate interest

Personal Data can also be processed if it is necessary to enforce a legitimate interest of any company belonging to the APR Group. Legitimate interests are generally of a legal (e.g. filing, enforcing or defending against legal claims) or financial (e.g. valuation of companies) nature.

Personal Data may not be processed based on a legitimate interest if, in individual cases, there is evidence that the interests of the employee merit protection. Before data is processed, it must be determined whether there are interests that merit protection.

Control measures that require processing of employee data can be taken only if there is a legal obligation to do so or there is a legitimate reason. Even if there is a legitimate reason, the proportionality of the control measure must also be examined. The justified interests of the company in performing the control measure (e.g. compliance with legal provisions and internal company rules) must be weighed against any interests meriting protection that the employee affected by the measure may have in its exclusion, and cannot be performed unless appropriate.

The legitimate interest of the company and any interests of the employee meriting protection must be identified and documented before any measures are taken. Moreover, any additional requirements under national law (e.g. rights of co-determination for the employee representatives and information rights of the data subjects) must be taken into account.

2.5 Automated Decisions

The APR Group may Process automatically Personal Data as part of the employment relationship (e.g. as part of personnel selection or the evaluation of skills, profiles and specific personal details are evaluated). In such event, the automatic Processing cannot be the sole basis for decisions that would have negative consequences or significant problems for the affected employee.

To avoid erroneous decisions, the automated process must ensure that a natural person evaluates the content of the situation, and that this evaluation is the basis for the decision. The Data Subject must also be informed of the facts and results of automated individual decisions and the possibility to respond.

2.6 Telecommunications and Internet

The APR Group provides its employees with telephone equipment, e-mail addresses, internet along with internal social network with the primarily aim to facilitate their job assignments. They are a tool and a company resource. They can be used within the applicable legal regulations and internal APR Group policies. In the event of authorized use for private purposes, the laws on secrecy of telecommunications and the relevant national telecommunication laws must be observed if applicable.

There will be no general monitoring of telephone and e-mail communications or intranet/internet use.

Nonetheless, to prevent attacks on IT infrastructure of the APR Group or to single employees' personal computer, protective measures can be implemented and this may involve the temporary logging of e-mail addresses, internet and social network. In such event, the evaluation of these data can be made: i) only by a qualified person, ii) ensuring that the principle of proportionality is met, iii) only in the event of concrete risk of attacks or damages for the APR infrastructure or, in general, iv) in the concrete risk of crime. In such event, the evaluation shall be made in full adherence with the applicable local laws and the GDPR.

3. THIRD PARTY DATA

3.1 Third Party Data

The APR Group may collect Personal Data customers, suppliers, consultants, partners and third parties in general, for the following reasons:

- **Providing Information and Services Requested.** The APR Group may collect and Process Personal Data to provide Individuals with information that may be requested, (e.g., but not limited to, information about a product or program the APR Group is offering). APR Group may also use Personal Data to deliver a specific program or service, when Individuals enroll to receive the program or service. Such use may include: (a) generally managing information; (b) responding to questions, comments and requests; (c) providing access to certain areas and features of the Sites and (d) registration for events.
- **Administrative Purposes.** The APR Group may use Personal Data for its administrative purposes, including, without limitation, to: (a) measure interest in Site, programs or services; (b) perform internal quality control; (c) verify identity; (d) send communications regarding the APR Group, programs or services, or any changes to any APR Group policy or terms of service; (e) process payments; (f) prevent potentially prohibited or illegal activities; and (g) enforce its policies.
- **Regulatory Purposes.** The APR Group may use Personal Data to comply with regulatory or legal requirements, including to investigate and report on adverse effects that might be experienced when using APR Group products.
- **Marketing and Commercialization.** The APR Group may use the Personal Data to inform its marketing and commercialization activities, including providing materials about offers, products and services offered, including new content or services on Sites. The APR Group may provide Individuals with these materials by postal mail, facsimile or email, as permitted by applicable law.
- **Research and Development.** The APR Group may use Personal Data to create non-identifiable information that the APR Group may use alone

or in the aggregate with information obtained from other sources, in order to help to optimally develop new products, processes and services.

- **Data Submitted Via Sites.** The APR Group may collect data through its Sites in order to provide services or respond to queries of guests of its Sites. In such event, Data Subject must be informed in relation to the collection, the Processing, the purposes of the Processing, the rights recognized by the applicable laws (and in particular by GDPR) through specific privacy policies. Such policies must contain also information in relation to the cookies, if any (please, refer to following Section 3.2)
- **Sharing Content with Friends or Colleagues.** APR Group's Sites may offer various tools and functionality. For example, the APR Group may provide functionality on its Sites that will allow Individuals to forward or share certain content with a friend or colleague.
- **Other Uses.** The APR Group may use Personal Data for other purposes disclosed to Individual at the time they voluntarily provided such information.

3.2 Social Media and Internet

Online social media resources are interactive tools that enable Individuals to collaborate and share information with others. Social media resources include, but are not limited to, social networks, discussion boards, bulletin boards, blogs, emails newsletter and referral functions to share Sites contents and tools with third parties (friends, colleagues, etc.).

The APR Group may collect Personal Data to enable Data Subjects to use online social media resources offered by the APR Group. The APR Group may also enable Individuals to use these social media resources to post or share Personal Data with others. Policies adopted by the APR Group on its Sites, specifies that, when using social media resources, Individuals must take into careful consideration what Personal Data they share with others.

When APR Sites offer online social media resource provided by a third party, the Sites must inform that the APR Group is not responsible for the

collection of the Personal Data eventually made by such third party and must invite Individuals to carefully read the related third party privacy policy.

The APR Sites may employ a cookie, or small piece of computer code that enables web servers to “identify” the guests of the Sites, each time an Individual initiates a session on the Sites. A cookie is set in order to identify Data Subjects; tailor the Sites; measure and research the effectiveness of Sites’ features, offerings and advertisements; and authenticate users for registered services. Cookies policies are available on the Sites and they inform the guests of the Sites on how they work and for which purpose they are used.

3.3 Consent to Process

The APR Group guarantees that no Personal Data is collected and/or Processed without the prior consent of the Data Subject.

Before giving consent, the Data Subject must be informed in accordance with this Policy. The declaration of consent must be obtained in writing or electronically for the purposes of documentation. In some circumstances, such as telephone conversations, consent can be given verbally. The granting of consent must be documented.

4. DATA TRANSMISSION

4.1 Transmission of the Data

The APR Group may, for business reasons, transfer Personal Data to third parties service providers. In such event, the transmission of Personal Data to third parties is subject to specific authorization requirements. Such transmission shall have to comply with the limits and principles of this Policy and must be in full adherence with the applicable laws (in particular with the GDPR in all the event the Data Subject is an European citizen) and must be done only for the purposes declared at the moment the permission to such transmission have been granted by the Data Subject.

If the transmission is made between two countries, the company of the receiving country must assure a protection of the data with a level at least similar to the one applied in the transmitting country and the data must be processed in accordance with this Policy, the applicable laws (including the GDPR when applicable).

4.2 Processing by third parties

Data collected by the APR Group, may be Processed on behalf of APR by a third party. In such event, the Processing by such third party must be:

- a) Ruled by a specific agreement;
- b) In full adherence and accordance with this Policy, the applicable laws and, in particular, the GDPR (when applicable);
- c) Previously authorized (in writing or electronically) by the Data Subject and the Data Subject must be informed in relation to the purposes of

the Processing, its rights according to the applicable laws and the GDPR.

In the event an APR Group company has the necessity to enter into an agreement that involves the Processing of Personal Data by a third party, such company must ensure that the following requirements are met:

- a) The provider of the service must be selected on the base of its ability to cover the required technical and organization protective measures;
- b) The agreement must be in writing and must contain a detailed description on the data Processing;
- c) The company must periodically check that the third party provider complies with its duties.

In the event the transmission of the Personal Data is cross border, the company must be sure that relevant applicable requirements for the disclosing of Personal Data abroad are met. In particular, Personal Data from European Economic Area can be processed in a third country only if the provider can prove that it has adopted data protection standard equivalent to this Policy.

5. DATA SUBJECT RIGHTS

The APR Group assures to any Individual that has grant its permission to Process its Personal Data, all the rights recognized by the applicable laws and, in particular, by the GDPR when applicable. Specifically, the APR Group recognizes, among the others, the following rights:

a) Notwithstanding the collection of Personal Data is made by the APR Group on voluntary base and only if previously authorized by the Data Subject, the Data Subject may request in anytime information related to which kind of data has been collected, stored and Processed and for what purpose.

b) Data Subject may require to know the identity of the third party to which its Personal Data has be transmitted (if applicable).

c) Data Subject can require the correction or the update of its data in any time.

d) Data Subject can obtain a limitation to the use of its data in any time.

e) Data Subject can object to the Processing of its data in any time. If the objection to the processing may affect the purpose for what such data has been originally collected (for example, to start a business collaboration) it must be immediately informed and it must be made aware that the eventual objection may prevent the prosecution of the business/employment relationship (if any).

f) Data Subject can exert any right recognized by the applicable laws and, in particular, by GDPR.

6. CONFIDENTIALITY

The APR Group does not allow any unauthorized collection, Processing, or use of Personal Data.

No APR Group employee and/or collaborator nor third parties, can have access to Personal Data collected by the APR Group if not expressly authorized in such way.

The APR Group maintains any data collected strictly confidential and limit the access to such data to the person that need to know them for the purpose such data have been collected.

The APR Group company that collected, for any of the reason specified under this Policy or if so required by the applicable law, is also responsible to maintain such data confidential and to protect them from unauthorized use.

The employees of the APR Group that have access for reasons related to their job to data collected by the APR Group, may not use such data, or communicated such data to third parties.

The APR Group also assures that any Personal Data collected is safeguard from unauthorized access and unlawful Processing or disclosure, as well as accidental loss, modification or destruction. This regardless such Data is Processed electronically or in paper form.

The APR Group applies the state of the art measures to protect data collected.

7. POLICY COMPLIANCE

APR verify the compliance with this Policy periodically through audits conducted by a specific team entrusted by APR and named the Compliance Board. The results of the periodic audit are referred in report that are provided to the CEO of APR and filed in APR archive.

In the event of non-compliance situations, specific actions are adopted by the Group CEO pursuant to the indications of the Compliance Board entrusted for the audit.

In certain case, in the event the non-compliance situation is due to behavior of single employees that do not respect this Privacy Policy, specific remedy/sanction against such employees may be adopted in accordance to the applicable laws of the country where the person is employed.

Any employee is required to inform its superior or the corporate legal department of APR, in the event he/she becomes aware of violation of this Privacy Policy or policies adopted by the related APR Group company as consequence of this Policy.

The superior or the corporate legal department shall immediately inform the Group CEO that shall adopt the measures that shall believe adequate for the case.

In the event of:

- Improper transmission of data to third parties;
- Improper access to data collected by the APR Group by third parties;
- Loss of data;

a report must immediately been prepared and provided to the Group CEO of APR in order to adopt the necessary measures and any reporting duties under the applicable national laws can be implemented.

7.1 Responsibilities and Sanctions

Any APR Group country manager is responsible for the application of this Policy in its subsidiary company and it is responsible to assure that the legal requirements of this Policy are met and that any data Processing activity is performed in compliance with this Policy.

If the complexity of the company or the particular nature of the business or of the data to be processed requires so, the country manager may require to the APR legal department specific advices in order to the application of this Privacy Policy.

Any country manager must be sure that its employees become familiar with this Privacy Policy.

Any country manager must inform its employees that improper use of data collected, and in general activities in violation of this Policy, can lead to sanctions under the applicable employment laws and, in the event of unauthorized exploitation of data collected or violation of the data protection laws, such action can be criminally prosecuted.

7.2 Contacts

As of the date of this Policy, APR has appointed as Data Protection Officer at both Corporate and European level its Corporate Director of Legal Department. Accordingly, any question in relation to the interpretation or application of this Privacy Policy may be submitted to the following address:

APR Applied Pharma Research s.a.
Corporate Legal Department
Via Corti 5
Balerna (CH) – 6828
Tel. +41 916957020
Fax. +41 916957029
e-mail privacy@apr.ch