neuromed CENTRU DE DIAGNOSTIC IMAGISTIC
Powered by SIEMENS
B-dul 16 Decembrie 1989 nr.43, 300218 Timișoara ■ Tel. +40-256-292637, 494403, 490182, 490185, Fax. +40-256-494403
www: neuromed.ro ■ e-mail: office@neuromed.ro

PERSONAL DATA PROTECTION POLICY

Table of contents:

B-dul 16 Decembrie 1989 nr.43, 300218 Timișoara ■ Tel. +40-256-292637, 494403, 490182, 490185, Fax. +40-256-494403
www: neuromed.ro ■ e-mail: office@neuromed.ro

1. Introduction

1.1 The background of the General Data Protection Regulation ("GDPR")

The General Data Protection Regulation, 679/2016, replaces the 1995 EU Data Protection Directive and the legislation of each Member State that has been drafted in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living persons) and to ensure that personal data are not processed without their knowledge and, whenever possible, that they are processed with their consent.

1.2 Definitions used by the organization (excerpts from GDPR)

Material scope (Article 2) - GDPR applies to the processing of personal data wholly or partly by automated means and to the processing by non-automated means of personal data that form part of a filing system or are intended to form part of a filing system.

Territorial scope (Article 3) - GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place within the Union or not. This Regulation applies to the processing of personal data of data subjects who are located in the Union by a controller or processor not established in the Union, where the processing activities are related to:

a) The offering of goods or services to such data subjects in the Union, irrespective of whether a payment of the data subject is required; or

b) The monitoring of their behaviour as far as their behaviour takes place within the Union. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

1.3 Definitions of Article 4

"Main establishment" - the main establishment of the controller in the EU shall be the place where the controller adopts the main decisions regarding the purpose and means of its data processing activities. The main establishment of a processor in the EU shall be its administrative centre.

"Personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to his or her own physical, physiological, genetic, mental, economic, cultural or social identity.

B-dul 16 Decembrie 1989 nr.43, 300218 Timișoara ■ Tel. +40-256-292637, 494403, 490182, 490185, Fax. +40-256-494403
www: neuromed.ro ■ e-mail: office@neuromed.ro

"Special categories of personal data" - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and genetic data processing, biometric data for the sole purpose of identifying a natural person, health data or data on the sexual life or sexual orientation of a natural person.

"Controller" means the natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

"Data subject" - any living person who is the subject of personal data held by an organization.

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

"Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

"Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

"Consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

"**Child"** is defined under GDPR as any person under the age of 16, although this may be reduced to 13 by the Member States' legislation. The processing of personal data of a child is legal only if the consent of their parents or guardians has been obtained. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child.

"Third party" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

"Filing system" means any structured set of personal data that are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

2. Privacy policy

2.1. The Board of Directors and the management of *SCM Neuromed*, with its headquarters in B-dul 16 Decembrie 1989 nr. 43, Timisoara, undertakes to comply with all relevant EU and Member State laws on personal data and the protection of the "rights and freedoms" of persons whose data *SCM Neuromed* collects and processes in compliance with the General Data Protection Regulation (GDPR).

B-dul 16 Decembrie 1989 nr.43, 300218 Timișoara ■ Tel. +40-256-292637, 494403, 490182, 490185, Fax. +40-256-494403
www: neuromed.ro ■ e-mail: office@neuromed.ro

2.2. The compliance with the GDPR is described by this policy and other relevant policies, such as the Information Security Policy (PIMS), along with the related processes and procedures.

2.3. The GDPR shall be applied by all persons at *SCM Neuromed* that process personal data, including all persons at *SCM Neuromed* that process the personal data of customers, employees, vendors and partners, as well as any other personal data the organization processes from any source.

2.4. The Data Protection Officer is responsible for the annual review of the **Records of processing activities** regarding any changes to the activities of *SCM Neuromed* (determined by changes recorded in the data mapping register) and by any additional requirements identified via data protection impact assessments. This register must be available upon the request of the supervisory authority.

2.5. This policy applies to all employees/staff members [and stakeholders] of *SCM Neuromed*, such as outsourced suppliers. Any violation of the GDPR shall be treated in accordance with the disciplinary policy of *SCM Neuromed* and may also represent a contravention, in which case the matter shall be reported as soon as possible to the competent authorities.

2.6. Partners and any third parties working with or for *SCM Neuromed* and who have or may have access to personal data are expected to have read, understood and complied with this policy. No third party may access the personal data held by *SCM Neuromed* without having previously concluded a data privacy agreement, which imposes on the third party obligations no less onerous than those that *SCM Neuromed* complies with, and that entitles *SCM Neuromed* to check the compliance with the agreement.

3. **Responsibilities** and **roles** under **the General Data Protection Regulation**:

3.1 *SCM Neuromed* is a [controller and/or processor] under the GDPR.

3.2 The senior management and all those with management or supervisory roles within the Organization are responsible for developing and encouraging data management practices within the Organization; the responsibilities are set out in the individual job descriptions.

3.3 The job description and the summary of tasks for the Data Protection Officer, a role specified in the GDPR: the DPO is a member of the management team, reports to the Organization's Board of Directors in regard to the management of personal data at *SCM Neuromed*, and ensures that the compliance with the data protection legislation and good practices can be demonstrated. This responsibility includes:

3.3.1 the development and implementation of this policy in line with the GDPR and

3.3.2 The management of security and policy compliance risks.

3.4 The **Data Protection Officer** has been appointed, being considered by the Board of Directors as qualified and having the appropriate experience to assume responsibility for the continued compliance of *SCM Neuromed* with the policy, and, in particular, the GDPR, as is the president, with regard to the data processing performed in their area of responsibility.

3.5 The Data Protection Officer has specific responsibilities with regard to procedures, such as the data subject's access request procedure, and is the primary contact for employees/staff members seeking clarification on any data protection compliance issue.

3.6 The compliance with the data protection legislation is the responsibility of all employees of *SCM Neuromed* that process personal data.

3.7 The training policy of *SCM Neuromed* sets out the specific training and awareness requirements for *SCM Neuromed* employees in relation to their specific data protection roles.

3.8 The Organization's employees/staff members are responsible for ensuring that the personal data they have provided to *SCM Neuromed* are accurate and up-to-date.

4. Personal data processing principles

The processing of personal data must be carried out in accordance with the data protection principles laid down in Article 5 of the GDPR. The *SCM Neuromed* policy and procedures are designed to ensure compliance with such principles.

4.1 Personal data must be processed **legally, fairly and transparently**

Legally - Identify a legal basis before processing the personal data. These are often referred to as "processing conditions", such as consent.

Fairly - In order for the processing to be conducted fairly, the controller is required to make some data available to the data subjects as practically as possible. This applies if the personal data have been obtained directly from the data subject or from other sources.

"**Transparently**" - GDPR includes rules on providing confidentiality information to the data subjects in Articles 12, 13 and 14. These are detailed and specific, emphasizing that notices concerning the data's privacy are understood and accessible. The information must be communicated to the data subject in an intelligible form using clear and simple language.

The specific information to be provided to the data subject must include at least:

4.1.1 **the identity and the contact details of the controller** and, where applicable, of the controller's representative;

4.1.2 the contact details of the **data** protection officer, where applicable;

4.1.3 **the purposes of the processing** for which the personal data are intended as well as the legal basis for the processing;

4.1.4 **the period** for which the personal data shall be stored;

4.1.5 **the existence** of the right to request access to, rectification, erasure or opposition to the processing, and the conditions (or lack of) to exercise such rights, such as affecting the legality of previous processing;

4.1.6 **the categories of personal data** concerned;

4.1.7 **the recipients** or categories of recipients of the personal data, if any;

4.1.8 where applicable, that the controller intends to **transfer** personal data to a recipient in a third country, as well as the ensured data protection level;

4.1.9 any additional information necessary to ensure proper processing.

4.2 Personal data may only be collected for specific, explicit and legitimate purposes

The data obtained for the specified purposes should not be used for purposes other than those that have been formally notified to the supervisory authority as part of the Record of processing activities of *SCM Neuromed*.

4.3 Personal data must be appropriate, relevant, and limited to what is required for processing

4.3.1 The Data Protection Officer is responsible for ensuring that *SCM Neuromed* does not collect data that is not strictly necessary for the purpose for which it is obtained (see DPIA Data Flow / Mapping Tool).

4.3.2 All data collection forms (electronic or paper), including data collection queries in new computer systems, must include a fair processing statement or a link to the privacy policy approved by the Data Protection Officer.

4.3.3 The Data Protection Officer shall make sure that, annually, all methods of data collection are reviewed by [internal audit / external experts] to ensure that the data collected are still appropriate, relevant and limited.

4.4 Personal data that are inaccurate, for the purposes for which they are processed, shall be erased or rectified without delay ("accuracy")

4.4.1 The data that is stored by the controller should be reviewed and updated as appropriate.

4.4.2 The Data Protection Officer has the responsibility to ensure that all staff members are trained in regard to the importance of collecting and maintaining accurate data.

4.4.3 It is also the responsibility of the data subject to make sure that the data held by *SCM Neuromed* are accurate and up-to-date. The filling in of a registration or request form by a data subject shall include a statement that the data contained therein are correct on the filing date.

4.4.4 Employees/customers etc., must notify *SCM Neuromed* of any changes to allow the proper updating of personal records. Instructions for updating the records: It is the responsibility of *SCM Neuromed* to make sure that any notification of changes is recorded and performed.

4.4.5 The Data Protection Officer is responsible for ensuring that the appropriate procedures and policies are in place to keep the personal data accurate and up-to-date, taking into account the amount of data collected, the speed at which such data may change, and any other relevant factors.

4.4.6 At least once a year, the Data Protection Officer shall review the retained data of all data subjects, which have been processed by *SCM Neuromed*, and kept in the data inventory, and it shall identify any data that are no longer required for the registered purpose. Such data shall be erased/destroyed in a safe manner in compliance with the procedure for the safe removal/destruction of storage media.

4.4.7 The Data Protection Officer is responsible for answering the rectification requests sent by data subjects within one month (the data subject's access request procedure). This term can be extended to two more months for complex requests. If *SCM Neuromed* decides not to comply with the request,

the Data Protection Officer must send a reply to the data subject explaining the reason and inform them about their right to file a complaint with the Supervisory Authority and to seek legal remedy.

4.4.8 The Data Protection Officer is responsible for taking the appropriate measures that, if third parties have received inaccurate or out-dated personal data, inform them that they are inaccurate and/or expired and should not be used; the Data Protection Officer is also responsible for submitting any personal data correction to the third party, if necessary.

4.5 Personal data must be kept in a form that allows the identification of the data subject only as long as necessary for processing.

4.5.1 If the personal data are kept beyond the processing date, such data shall be [minimized / encrypted / pseudonymized] to protect the identity of the data subject in the case of a data breach.

4.5.2 Personal data shall be retained in accordance with the record keeping procedure and, once the retention date has been exceeded, these data must be destroyed in a safe manner, as required by this procedure.

4.5.3 The Data Protection Officer must specifically approve any storage of data that exceeds the retention periods defined in the Record Keeping Procedure, and must make sure that the justification is submitted in a clear manner and in accordance with the legal data protection requirements. This approval shall be obtained in writing.

4.6 Personal data must be processed in a manner that ensures their proper security

The Data Protection Officer shall perform a risk assessment, taking into account all the circumstances of the processing operations of *SCM Neuromed*.

In determining adequacy, the Data Protection Officer should also take into account the extent of any damage or loss that might be caused to persons (e.g. staff or customers) in the event of a security breach, the effect of any security breach on *SCM Neuromed*, and any possible reputational damage, including possible loss of customer trust.

When assessing the appropriate technical measures, the Data Protection Officer shall take into account at least the following:

- Password protection;
- Automatic lock of terminals (computer/laptop etc.) when not in use (idle state);
- The removal of access rights for USB and other storage media;
- Anti-virus software and firewalls;
- Role-based access rights, including those assigned to temporary staff;
- The encryption of devices leaving the organization's premises, such as laptops;
- Local and WAN network security;
- Privacy Enhancement Technologies, such as **pseudonymization** and anonymization;
- The identification of international security standards relevant to *<organization name>*.

When assessing appropriate organizational measures, the Data Protection Officer shall also take into account the following:

- The appropriate training levels within the Organization;
- The inclusion of data protection measures in employment contracts;
- The identification of disciplinary actions for data breaches;
- The monitoring of the compliance of staff members with the relevant security standards;
- The control of physical access to electronic and paper records;
- The storage of paper-based data in secured cabinets;
- The restriction on the use of portable electronic devices outside the workplace;
- The restriction on the use of the employee's personal devices at work;
- The adoption of clear rules on passwords;
- The regular backup of personal data
- Impose contractual obligations on importers to take appropriate security measures when transferring data outside the EEA.

Attention should be paid to the data processing risks, which can cause damage to the data subjects whose data are processed.

4.7 The controller is required to be able to demonstrate compliance with the other GDPR principles (accountability)

The GDPR includes provisions that promote accountability and governance. These supplement the transparency requirements of the GDPR. The principle of accountability under Article 5(2) requires the controller to demonstrate that they comply with the principles and explicitly state that this is the controller's responsibility.

SCM Neuromed shall demonstrate compliance with the data protection principles by implementing data protection policies, the compliance with the codes of conduct, by implementing technical and organizational measures, and by adopting techniques such as data protection from conception, DPIA, notification procedures for breaches and incident response plans.

5 Rights of the data subjects

5.1 The data subjects have the following rights in regard to the data processing and recording of such data:

5.1.2 The right of access to the data held and relating to the recipients such data may have been disclosed to;

5.1.3 The right to object to the processing that could cause damage or prejudices;

5.1.4 The right to object to the processing for the purpose of direct marketing;

5.1.5 The right to be informed about automated individual decision-making, including profiling;

5.1.6 The data subject has the right not to be the subject to a decision based solely on automatic processing, including profiling, which produces legal effects affecting the data subject or similarly affecting him or her to a significant extent;

5.1.7 The right to claim damages if they suffer damages through any violation of the GDPR;

5.1.8 The right to take action for the rectification, blocking, deletion, including the right to be forgotten or the destruction of inaccurate data;

5.1.9 The right to request the Supervisory Authority to assess whether a GDPR provision has been violated;

5.1.10 The data subject has the right to receive their personal data, which they have provided to the controller, in a structured, commonly used way, and which can be read automatically, as well as the right to send such data to another controller without any obstacles from the controller to whom such personal data have been provided;

5.1.11 The data subject has the right to object to the creation of profiles without their consent.

5.2 *SCM Neuromed* guarantees that the data subjects can exercise these rights:

5.2.2 Data subjects may submit requests to access their data, in accordance with the Data Subject Access Procedure; this procedure also describes how *SCM Neuromed* shall ensure that its response to the data access request complies with the GDPR requirements.

5.2.3 Data subjects have the right to lodge a complaint against *SCM Neuromed* in connection with the processing of their personal data; the requests received from the data subjects and the complaint solving method shall comply with the Complaints procedure.

6 Consent

6.1 *SCM Neuromed* understands that the "consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The data subject may withdraw his or her consent at any time.

6.2 *SCM Neuromed* understands that the "consent" of the data subject means they have been fully informed about the processing of personal data, and that they have given their consent while in a state appropriate to do so and without being pressured. The consent obtained under pressure or based on misleading information shall not constitute a valid basis for processing.

6.3 There must be active communication between the parties to demonstrate active consent. The lack of response to a communication does not mean consent has been given. The controller is required to be able to demonstrate consent to the processing operation.

6.4 For sensitive data, an explicit written consent of the data subjects has to be obtained, unless there is a legal basis for alternative processing.

6.5 In most cases, the consent to the processing of sensitive and personal data is typically obtained by *SCM Neuromed* using standard consent forms.

6.6 If *SCM Neuromed* provides online services to children, the consent of the child's parent or legal guardian must be obtained. This requirement applies to children under the age of 16 (unless the Member State provides for a lower age limit, which may not be less than 13).

7 Data security

7.1 All employees/staff members are responsible for ensuring that all personal data *SCM Neuromed* holds and is responsible for are kept safely and are not disclosed in any way to third parties, unless that third party has been specifically authorized by *SCM Neuromed* to receive such information and has concluded a confidentiality agreement.

7.2 All personal data should only be accessible to those who need to use it, and access can only be granted in compliance with the Access Control Policy. All personal data must be processed in a safe manner and must be kept:

- in a locked room with controlled access; and/or

- in a locked drawer or cabinet; and/or
- if kept on computers, these have to be password-protected, in compliance with the organization's requirements listed in the Access Control Policy; and/or
- stored on (removable) media that are encrypted.

7.3 Care must be taken to ensure that the screens and PC terminals are only visible to the employees/authorized personnel of *SCM Neuromed*. All employees/staff members are required to enter into an acceptable use agreement before being allowed access to organizational data of any kind, detailing the rules applicable when the screen is idle (locked).

7.4 Physical records cannot be stored in locations where they can be accessed by unauthorized personnel, and cannot be removed from the premises without explicit [written] authorization. As soon as physical records are no longer required for daily clients, such records must be destroyed in a safe manner, in accordance with a specific procedure.

7.5 Personal data can only be deleted or removed in compliance with the record keeping procedure. Physical records that reached their expiration date must be shredded and discarded as "confidential waste".

7.6 The processing of personal data "off-site" poses a potentially greater risk OF loss, theft or damage to personal data. The staff members must be specifically authorized to process the data off-site.

8 Disclosure of data

8.1 *SCM Neuromed* must make sure that personal data is not disclosed to unauthorized third parties, including family members, friends, and government bodies and, under certain circumstances, the Police. All employees/staff members must be careful when asked to disclose personal data held by another person to a third party [they shall be required to participate in specific training that will enable them to manage such risks effectively]. It is important to take into account whether the disclosure of data is or is not relevant to the activity of *SCM Neuromed.*

8.2 The GDPR allows certain cases of disclosure without consent as long as the information is required for one or more of the following purposes:

8.2.1 - to safeguard national security;

8.2.2 - to prevent or identify offenses, including the criminal detention or prosecution of offenders;

8.2.3 - to perform regulatory functions (including health, safety and well-being of people at work);

8.2.4 - to prevent serious injury to a third party;

8.2.5 - to protect the vital interests of the natural person; it refers to life and death situations.

8.3 All data disclosure requests for one of these reasons must be supported by appropriate documentation, and all such disclosures must be specifically authorized by the Data Protection Officer.

9 Data storage and erasure

9.1 *SCM Neuromed* shall not retain personal data in a form that allows the identification of data subjects for a longer period than necessary in relation to the purpose(s) for which such data has been originally collected.

9.2 *SCM Neuromed* may store data for longer periods if personal data are processed exclusively for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes, subject to the implementation of appropriate technical and organizational measures to protect the rights and freedoms of the data subject.

9.3 The retention period for each category of personal data shall be defined in the Record Keeping Procedure along with the criteria used to determine this period, including the legal obligations of *SCM Neuromed* retaining the data.

9.4 The data retention and data erasure procedures of *SCM Neuromed* shall apply in all cases.

9.5 Personal data must be safely disposed of in accordance with the sixth principle of the GDPR - processed in an appropriate manner to maintain their security, thus protecting the "rights and freedoms" of the data subjects. Any data erasure shall be carried out in accordance with the erasure procedure.

10 Data transfers

10.1.1 All data transfers from the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as "third countries") are illegal, unless there is an "adequate level of protection of the fundamental rights of the data subjects".
The transfer of personal data outside the EEA is prohibited, unless one or more specified safeguards or exceptions apply:

10.1.2 The existence of an adequacy decision
The transfer of personal data to a third country or an international organization may be performed when the Commission has decided that the third country, territory or one or more specified sectors from that third country or international organization ensures an adequate level of protection. Transfers under these conditions do not require special authorizations. Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as fulfilling the conditions of the adequacy decision.
A list of countries currently fulfilling the Commission's adequacy requirements is published in the Official Journal of the European Union. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

10.1.3 Privacy Shield
If *SCM Neuromed* wants to transfer personal data from the EU to a US organization, it should check if the organization is registered with the Privacy Shield administered by the U.S. Department of Commerce. The obligation applicable to companies registered with the Privacy Shield is included in the Data Privacy Principles. The U.S. Department of Commerce is responsible for managing and administering the Privacy Shield, and for ensuring that organizations honour their commitments. In order to be certified, companies must have a privacy policy complying with the data privacy principles, e.g. use, storage and transfer of personal data, in accordance with a strong set of rules and data protection safeguards. The protection of personal data applies irrespective of whether the personal data is related to an EU resident or not. Organizations need to renew their Privacy Shield "membership status" every year. If they fail to do so, they can no longer receive and use personal data from the EU.

Controller adequacy assessment
When assessing adequacy, the controller transferring UK data should take into account the following factors:

- the nature of the data transferred;
- the country or territory of origin and the final destination of the data;
- how the data shall be used and for how long;

- the laws and practices of the transferee's country, including relevant data protection practices and international obligations; and
- the security measures to be taken with regard to externally located data (valid for UK only).

10.1.4 Mandatory corporate rules

SCM Neuromed may adopt binding corporate rules for data transfers outside the EU. This requires submitting for approval to the competent supervisory authority the rules that *SCM Neuromed* is trying to rely on.

10.1.5 Standard contract clauses

SCM Neuromed may adopt approved contractual standard clauses for data transfers outside the EEA. If *SCM Neuromed* adopts [the standard contract clauses approved by the competent supervisory authority] then there is an automatic recognition of adequacy.

10.1.6 Exceptions

In the absence of an adequacy decision, Privacy Shield membership, mandatory corporate rules and/or standard contract clauses, the transfer of personal data to a third country or an international organization shall take place only under the following conditions:

- the data subject explicitly agreed to the proposed transfer after having been informed of the possible risks of such transfers to the data subject, due to the lack of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or for the implementation of the pre-contractual measures taken at the request of the data subject;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary to protect the vital interests of the data subject or other persons, in cases where the data subject is not physically or legally capable of giving consent.

11 The record of processing activities and the data mapping system

11.1 *SCM Neuromed* has set up a Record of processing activities and DATA MAPPING System as part of its strategy to address the risks and opportunities within its GDPR Compliance Project. The record of processing activities and data mapping system refers to:

- processes that use personal data;
- the source of personal data;
- the volume of data corresponding to the data subjects;
- the description of each personal data item;
- processing activities;
- maintaining the inventory of processed data categories;
- documenting the purpose(s) for which each category of personal data is used;
- recipients and potential recipients of personal data;
- the role of *SCM Neuromed* within the data flow;
- storage systems;
- any data transfer; and

- all requirements for storing and deleting personal data.

11.2 *SCM Neuromed* is aware of the risks associated with the processing of certain types of personal data.

11.2.1 *SCM Neuromed* assesses the risk level for the processing of the personal data of the data subjects. **Data Protection Impact Assessments (DPIAs)** are carried out taking into account the processing of personal data by *SCM Neuromed* and the processing performed by other organizations on behalf of *SCM Neuromed.*

11.2.2 *SCM Neuromed* must manage any risks identified by the risk assessment to reduce the probability of non-compliance with this policy.

11.2.3 Given the nature, scope, context and purposes of the processing, where a type of processing, especially the one based on the use of new technologies, is likely to create a high risk for the rights and freedoms of natural persons, the operator shall conduct, before processing, an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may target a set of similar processing operations that present similar high risks.

11.2.4 If the outcome of the DPIA reveals that *SCM Neuromed* is about to start processing personal data that could cause damage and/or prejudice to the data subjects, the decision to start the processing by *SCM Neuromed* shall rest with the Data Protection Officer.

11.2.5 The Data Protection Officer shall report this situation to the Supervisory Authority, if there are significant concerns, either in relation to damage and/or prejudices, or the volume of data.

11.2.6 Appropriate security standards [e.g.: ISO 27001, etc.] and their scope shall be applied to reduce the level of risk associated with the processing of individual data to an acceptable level.

Procedure approval

This document has been approved by the Data Protection Officer, who is also responsible for reviewing this procedure in accordance with the revised requirements of the General Data Processing Regulation (EU GDPR).

An updated version of this procedure is available to all members of the organization on www.neuromed.ro.

This policy has been approved by the Organization's Board of Directors on 23 May 2018 and issued as a revised version under the President's signature.

Signature Date: 23/05/2018

Procedure version and revision history:

Version	Revised component	Approval	Version date
1	Version 1	Chairman	23/05/2018