(To be filled out in the EDPS' office)
REGISTER NUMBER: 1473

(To be filled out in the EDPS' office)

NOTIFICATION FOR PRIOR CHECKING

DATE OF SUBMISSION: 11/09/2017

CASE NUMBER: 2017-0804

INSTITUTION: EC - DG SANTE

LEGAL BASIS: ARTICLE 27-5 OF THE REGULATION CE N° 45/2001([1])

INFORMATION TO BE GIVEN[2]

1/ NAME AND ADDRESS OF THE CONTROLLER

CONTROLLER : RYS ANDRZEJ JAN
E-MAIL:

DELEGATE : PIHA TAPANI

E-MAIL: Tapani.PIHA@ec.europa.eu

2/ ORGANISATIONAL PARTS OF THE INSTITUTION OR BODY ENTRUSTED WITH THE PROCESSING OF PERSONAL DATA

THE EUROPEAN COMMISSION
DG SANTE - DIRECTORATE DDG1.B

3/ NAME AND DESCRIPTION OF THE PROCESSING

NAME: Clinical Patient Management System (CPMS)

European reference networks (ERNs) for rare diseases are virtual networks bringing together healthcare providers across Europe to improve the diagnosis and treatment of patients with rare, low prevalence

[1] OJ L 8, 12.01.2001.

and complex diseases. They also serve as research and knowledge centres, updating and contributing to the latest scientific findings in the area of rare and complex diseases. The Networks are set up under Directive 2011/24/EU[1] of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare. The Directive requires the Commission to support Member States in the development of European reference Networks ("Networks") between healthcare providers and centres of expertise. The consent of the patient is dealt with in recital 12 of the Delegated Decision and the definition of the informed consent in Article 2 (e) of the Delegated Decision.

The Clinical Patient Management System (CPMS) is a Sofware as a Service (SaaS) that has the objective of supporting health professionals in the European Reference Networks to collaborate virtually in the diagnosis and treatment of patients with rare or low prevalence complex diseases or conditions across national borders in the European Union. The CPMS provides a web-based tool for the sharing and hosting of patient data with the explicit patient's consent and uses a secure electronic system – the authentication and identity management service (EU Login) and the SAAS2 – managed by the Commission to process personal data to authenticate and to authorise ERN users' access to the patient's files. The objective of the CPMS is to support ERN users to collaborate on the medical assessment of a patient file for treatment and diagnosis across national borders.

The purpose of this notification is to describe the processing of personal data within the context of the CPMS. In the context of this system, the European Commission is data controller of the personal data of users of the system and managers of the access rights of the CPMS. The Commission is also co-controller of patient data, because it provides the means to process patient data (including health data), although it does not determine its processing purposes. Neither the Commission, nor its contractors and subcontractors, have access, at any stage of the processing, to any patient data. A set of adequate safeguards has been implemented to that effect (see section 18). Notwithstanding, the pseudonymised (encrypted) patients' data is securely stored, on behalf of the Commission, by its subcontractor in Germany, solely to ensure the proper functioning of the CPMS platform.

The following data is processed by DG SANTE:

1. User data (for users and guest users)

This concerns personal data of the healthcare professionals to permit access to the CPMS tool. This data is requested, submitted, collected, stored and used for purposes of operating the system (e.g. how many active users are logged in the system for invoicing purposes) and in audit logs. There are two types of users in the CPMS: (i) local point of care specialists who belong to an ERN member hospital and treatment centre (known as "users") and (ii) local point of care specialists who belong to an affiliated or non-member hospital or treatment centre (known as "guest users"). Whereas users are given the full scope of access rights, the rights of guest users to perform actions in the system is attributed on a need-to-do basis by the responsible ERN coordinator. Guest users access rights can either: (i) be limited to enrolling a patient and filling in the consultation form. Then a Panel request will be forwarded to the ERN coordinator of the selected ERN to assign a Panel Lead and the regular workflow follows; or (ii) a guest user participates actively as a Panel member. This may be particularly useful for a patient enrolled by the guest user. It’s important to say that the data personal data collected for both users and guest users is exactly the same. Moreover, guest users cannot be Panel Leads in the CPMS. Before a user account is created in CPMS, any user must first create their own authenticated account in EU Login, the user authentication and identity management service[11] for the European institutions. CPMS user accounts are then authorised by the DG SANTE authorisation system SAAS2[12]. Only users who are authenticated and authorised are activated in CPMS and a component of SAAS, which is a local user

management tool, is used to reconcile authorised user lists from SAAS and deactivates any changes in users in CPMS on the basis of comparing EU Login ids. The user data stored by EU Login and SAAS, fall under the EU Login (1)/SAAS (2) privacy statements and their respective notifications to the DPO (EU Login DPO-839.4 and DG SANTE SAAS DPO-2065.4). See section 5 below for a description of the collected personal data categories. The personal data of the users is stored in databases hosted at the European Commission Data Centre. Access to modify user authentication data (EU Login) is open only to the users themselves. Modification of the authorisation user data in SAAS is on the basis of a request to European Commission authorized personnel via the authorisation system SAAS2. Besides storing these data in the aforementioned systems, the personal data in the CPMS is stored as well in the Software as a Service data hosting centre in Germany. The roles of the CPMS users are to enrol patients, collaborate in the assessment of pseudonymised patient files for treatment and diagnosis, with a secondary objective of using pseudonymised data for data registries or specific named research project subject to the patient's explicit consent. Said consent forms are kept by the treating doctor, who is responsible for handling consent and cannot proceed in the CPMS workflow without it. The consent form is not uploaded in the CPMS, but kept by the treating doctor (known as the point of care specialist) in the patients' file at local level. When introducing the patient's data in the CPMS system, the point of care specialist ticks a pop-up box confirming that consent has been given. A standard consent template is available from a download link in the CPMS (see Annex). It sets out the patients' rights, including how to give or withhold consent, and whom to contact for any information regarding the processing of data. It also provides a link to the CPMS specific privacy statement. Users of the system who enrol patients, do so in a an app that is securely and logically ring-fenced to contain the enrolment of a patient in one app (HCP app) in which the patient first name, last name and date of birth are entered by the local point of care specialist and instantly pseudonymised. This app encapsulates, for the local (point of care) specialist user, the logic and security rules required by the treatment centre and its patients. There is one instance of the HCP App per hospital or treatment centre. Only the pseudonymised data is passed to CPMS users for panel discussion and assessment of a patient file in a second app (ERN app). This guarantees that CPMS users can ensure that the patient is immediately pseudonymised on enrolment before being picked up by the panel for assessment of the patient file. The users of the patient data enter such data resorting to pseudonymisation safeguards (see section 18). .

2. Users managing access rights

Other data processed for the purpose of operating the system include data of personnel employed by the Commission, including intra- or extra-muros contractors, which is processed in a separated user management app, which is logically and securely ring-fenced.to be separated from patient data These users have accounts in this user management app and the rights to manage users of the CPMS (check that accounts are set up with the right details). These users are indicated as the responsible person for administrative purposes, and are included in the database amongst the users above; however, their contact details are not made available to the user community. Instead, a functional mailbox is used for facilitating contact between users and administrators (see section 10 of the attached Specific Privacy Statement).

See section 5 below for the collected personal data categories.

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1463060833116&uri=CELEX:32011L0024
[2] http://ec.europa.eu/health/rare_diseases/european_reference_networks/erf/
[3] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014D0286&from=EN
[4] http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014D0287&from=EN
[5] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0286&from=EN
[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML
[7] http://www.who.int/classifications/icd/en/

[8] http://www.orpha.net/consor/cgi-bin/Disease.php?lng=EN
[9] http://ec.europa.eu/health/ehealth/docs/com_2012_736_en.pdf
[10] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=en
[11] Notification to the DPO 839, including EU Login Privacy Statement
[12] Notification to the DPO 2065, including SAAS2 Privacy Statement

4/ PURPOSE OR PURPOSES OF THE PROCESSING, AND PROCESSORS

The objective of the clinical patient management system (CPMS) is to support ERN users to collaborate on the medical assessment of a patient file for treatment and diagnosis across national borders. This DPO notification concerns personal data of the users of the clinical patient management system (CPMS) to permit access for the users – the ERN health professionals – to collaborate with each other. This data is requested, submitted, collected, stored and used for purposes of operating the system and to identify users. This personal data is collected at system level and is used to manage the IT aspects of the system (user groups, access rights, monitoring of functioning of the system, support, maintenance, pay per use (for active users) for the software as a service.

PROCESSORS:
The third party processors include: The contractors (framework contract SANTE/2016/A4/013, c.f. award[1]) OpenApp Consulting Ltd and Vitro Software for the provision, maintenance and development of the CPMS and their sub-contractors and services providers, Microsoft Azure, Germany[2] and Osimis[3].
[1] Official Journal 2017/S 022-036631
[2] https://azure.microsoft.com/en-us/overview/clouds/germany/
[3] http://www.osimis.io/en/

5/ DESCRIPTION OF THE CATEGORY OR CATEGORIES OF DATA SUBJECTS

CPMS Users and Guest users: Healthcare professionals who are employed by European Reference Network member hospitals and healthcare professionals from an affiliated / non-member hospital or treatment centre. Users managing the access rights of CPMS: Personnel employed by the Commission, including intra- or extra-muros contractors, who manage the access rights of the CPMS users.

6/ DESCRIPTION OF THE DATA OR CATEGORIES OF DATA *(including, if applicable, special categories of data (Article 10) and/or origin of data).*

a) CPMS Users and Guest users: · EU Login username; · First and last names; · Organisation details (Healthcare provider name); · ERN username; · Professional e-mail address; · Country; (b) Users managing the access rights of CPMS: · EU Login username; · First and last names; · Organisation details; · ERN username; · Professional e-mail address; · Country;

7/ INFORMATION TO BE GIVEN TO DATA SUBJECTS

A Specific Privacy Statement for CPMS users and users managing access rights will be hyperlinked from the application (see attachment).

CPMS Information System

The ERN users / guest users of the CPMS cannot enrol or see even pseudonymized patient data unless unambiguous consent is provided by the patient or guardians/parents at enrolment of the patient in the CPMS.

8/ PROCEDURES TO GRANT RIGHTS OF DATA SUBJECTS

To exercise his or her data subject rights concerning CPMS, the user should contact the respective data controllers at the Commission by using the "Contact Information" regarding CPMS in the privacy statement or send an email to the functional email address on the log in page of the system. It must be underlined that, even when a user or guest user deletes or requests deletion of his/her profile from the CPMS, such deletion occurs only at EU Login level. At the CPMS, his/her account is merely deactivated, which means that certain personal data categories (first and last name and specialty) of users / guest users are still visible within the CPMS platform even after the account's deactivation. The same concerns any pseudonymised patient data that such user or guest user have imputed into the platform. The purpose is to ensure in the ongoing care of the patient or to contribute to the care and diagnosis of another patient. A CPMS healthcare professional (user) only has the right to enrol a patient based on explicit consent provided by the patient. The patient data can be wiped at the request of the patient (to their healthcare professional). In case the user / guest user account has been deactivated (or in any circumstance where the user / guest user is not in a position to exercise patient's data protection rights, e.g. death), the ERN coordinator has the possibility to perform this function.

9/ AUTOMATED / MANUAL PROCESSING OPERATION

Automated operations: User management data is used for user support and logs of activity that are stored, for as long as necessary, for evaluation and system monitoring purposes, on system servers hosted, as mentioned previously, for metrics (aggregated) and used by IT personnel (intra or extra-muros contractors of the European Commission to monitor the functioning of the system and payment of invoices). Aggregate statistics, not containing personal data, on the number of patients treated or diagnosed per ERN or per country or the number of specialists contributing, etc. will allow the European Commission to monitor the implementation and effectiveness of the European Reference Networks (as provided for in the legislation). Manual operations: Personal user data collected via EU Login can be manually modified and deleted by the user upon which it is no longer possible to log in to the CPMS. Alternatively access revocation can be requested by the user to the ERN coordinator or local treatment centre representative.

10/ STORAGE MEDIA OF DATA

Authenticated and authorised user / guest user details are stored in CPMS where rights are ascribed to the user access to collaborate on the medical assessment of a patient file for treatment and diagnosis across national borders. All data in the CPMS is hosted in the Commission's subcontractor data centre in Germany, with implemented standards on secure processing.
[1] https://ec.europa.eu/taxation_customs/about/privacy-statement-internet-website-commissions-taxation-customs-union-directorategeneral/privacy-statement_en
[2] http://ec.europa.eu/dpo-register/download?metaId=1474944
[3] http://ec.europa.eu/dpo-register/details.htm?id=42750
[4] http://ec.europa.eu/dpo-register/details.htm?id=43368

11/ LEGAL BASIS AND LAWFULNESS OF THE PROCESSING OPERATION

DIRECTIVE 2011/24/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 March 2011[1] on the application of patients' rights in cross-border healthcare, in particular Article 12 ("European Reference Networks"); COMMISSION DELEGATED DECISION of 10 March 2014[2] setting out criteria and conditions that European Reference Networks and healthcare providers wishing to join a European Reference Network must fulfil, in particular Recitals (8) (facilitation of health data exchange), (9) (processing of personal data), (12) (informed consent) and Article 2, in particular line (e) (definition of informed consent), as well as Annexes I and II (in particular point 1, regarding the latter, for the collection of patients' informed consent by applicant providers). COMMISSION IMPLEMENTING DECISION of 10 March 2014[3] setting out criteria for establishing and evaluating European Reference Networks and their Members and for facilitating the exchange of information and expertise on establishing and evaluating such Networks, in particular recitals 13 (facilitating the exchange of information) and 14 (compliance with Regulation 45/2001), as well as Article 16 ("Exchange of information on establishing and evaluating the networks"), in particular point (1)(d). COUNCIL RECOMMENDATION of 8 June 2009 on an action in the field of rare diseases (2009/C151/02); This processing operation is lawful under articles 4(1)(a) and 5, in particular point (a) and point (d) of Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. This processing operation does not fall under any of the categories foreseen in article 27 of Regulation 45/2001. No exemptions and restrictions foreseen in article 20 of Regulation 45/2001 apply to this processing operation.
[1]OJ – L88 of 4.04.2011
[2] C (2014) 1408 final
[3] C (2014) 1411 final

12/ THE RECIPIENTS OR CATEGORIES OF RECIPIENT TO WHOM THE DATA MIGHT BE DISCLOSED

Users and users managing access rights have access only to view and to directly modify (change or delete) their personal details. Guest users' access rights are defined by the ERN Coordinator upon their registration in the system on a need-to-do basis. They can be more limited than the rights given to users. A service directory of CPMS users, namely, healthcare professionals, is available to the authorised CPMS users / guest users,. This data is name, organisation (hospital or treatment centre),

ERN, country, area of specialisation (e.g. radiology). In this way, healthcare professionals in ERNs can build the most effective panels of relevant specialists to diagnose and care for patients. If necessary, in very specific cases (namely to exercise patients' rights, in cases where the responsible point of contact cannot do so), the ERN coordinator may be given access to certain areas of the platform and/or to the personal data of certain users.

13/ RETENTION POLICY OF (CATEGORIES OF) PERSONAL DATA

User data and patient data are retained in the CPMS as long as necessary in the interest of patient care and diagnosis and are hosted in the Commission's subcontractor data centre in Germany, with implemented standards on secure processing. 13.1 Access Management Systems Personal data recorded through the CPMS are retained for as long as necessary, e.g. if healthcare professional has contributed to the assessment of a patient file, but is no longer an active user, the user details will be retained but deactivated for as long as necessary in the interest of patient care and diagnosis. Guest users' accounts are active for 90 days by default from the date of registration, unless different requirements are needed. If that is the case, a shorter or longer end date can be set. Once the end date is reached, the guest user account is deactivated, and data is kept in exactly the same way as for users accounts. Patient data will be archived in a database within the CPMS and retained for further care purposes or the care purposes of family members. This data (which is uploaded into the CPMS with explicit patient consent only) may be used to generate disease registries by the ERNs, which are 'queries' or 'reports' on the data in the database for as long as necessary to ensure patient care and diagnosis. 13.2 CPMS System Administration Data Contact details of the users and responsible persons of the CPMS are kept in the system for as long as necessary and as long as the system is active. Contact details are deleted directly from the user or upon request by the user the system administrators as outlined in the specific privacy statement.

13 A/ TIME LIMIT TO BLOCK/ERASE ON JUSTIFIED LEGITIMATE REQUEST FROM THE DATA SUBJECTS

Personal data will be removed within four weeks from the receipt of the legitimate request from the data subject.

14/ HISTORICAL, STATISTICAL OR SCIENTIFIC PURPOSES

If you store data for longer periods than mentioned above, please specify, if applicable, why the data must be kept under a form which permits identification.

N/A

15/ PROPOSED TRANSFERS OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

N/A

16/ THE PROCESSING OPERATION PRESENTS SPECIFIC RISK WHICH JUSTIFIES PRIOR CHECKING

Article 27.2.(a) Processing of data relating to health and to suspected offenses, offenses, criminal convictions or security measures

17/ COMMENTS

PLACE AND DATE: BRUXELLES, 08.09.2017

DATA PROTECTION OFFICER: RENAUDIERE PHILIPPE

INSTITUTION OR BODY: THE EUROPEAN COMMISSION