

REGISTER NUMBER: 579

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 15/02/2010

Case number: 2010-089

Institution: ECDC
(2 different processing operations)

Legal basis: article 27-5 of the regulation CE 45/2001⁽¹⁾

⁽¹⁾ OJ L 8, 12.01.2001

INFORMATION TO BE GIVEN⁽²⁾

⁽²⁾ Please attach all necessary backup documents

1/ Name and address of the controller

Jessica MANNHEIM, Head of Human Resources Section; ECDC, SE-17183 Stockholm,
jessica.mannheim@ecdc.europa.eu

2/ Organisational parts of the institution or body entrusted with the processing of personal data

- > ECDC Administration Unit, Human Resources Section (as 'controller');
- > Feelgood Östermalmshälsan AB (Box 27301, SE-10254 Stockholm; corporate identity number 556185-6385 - as 'processor');
- > Aleris Medilab (Stockholm; corporate identity number 556052-8746 - as 'processor for the processor')

3/ Name of the processing

Annual medical examination

4/ Purpose or purposes of the processing

Diagnosis and prevention of illness

5/ Description of the category or categories of data subjects

ECDC Temporary Staff and Contract Staff

The data are collected from the data subjects themselves.

6/ Description of the data or categories of data including, if applicable, special categories of data (article 10) and/or origin of data)

A. Data categories:

1. Medical tests:

A) BASELINE

1. Medical history and complete physical examination.

2. Laboratory tests:

a. Hematology: Sedimentation rate, Red blood count, White blood count, Hemoglobin, Hematocrit, Platelets, (Thrombocytes), MCV, Faeces HB – For women and men 45 years and over

b. Blood chemistries: Creatinine, Uric acid, Glucose, Cholesterol and HDL, Triglycerides, Gamma GT, Transaminases (SGO/ASAT and SGP/ALAT)

c. Serology: HIV antibodies: this test may be carried out only after full information on the disease and consent as attested by the signature of the data subject.

d. Urine analysis: Sugar, Albumin, Microscopic examination (now done with sticks)

3. Standard chest X-Ray (when advised by the examining doctor).

4. Electrocardiogram at rest, and for persons over 45 years: exercise (stress) E.C.G. if any clinical suspicion, or risk factor.

5. EYE examination (compulsory every third year for drivers and videoscreen users working on a V.D.U. more than 4 hours daily): Visual acuity (distance and near) with and without glasses; Glaucoma screening (to be done by the optician)

B) FOR WOMEN OVER 25 YEARS: PAP-test

C) FOR WOMEN OVER 40 YEARS: PAP-test; Baseline mammogram every second year and if there is a specific risk the mammogram can be performed in women from 35 years on.

D) FOR MEN OVER 45 YEAR: P.S.A.

2. **'Certificate of Health'** (template attached herewith, Annex I), stating whether the data subject is 'in good health and fit for work, both mentally and physically'.

3. **Data subject identification data:** name, age, date of birth, personal identification number, nationality;

4. **Related administrative data:** medical appointments and payment of processor's services.

B. Description of personal data processing operation: staff members who are due for annual medical checks (the 'data subjects'), make, at the reminder of the controller (ECDC's Human Resources Section), an appointment with, and visit, the processor (Feelgood Östermalmshälsan AB), who examines them medically on behalf of the ECDC. The reminder specifies that the examination is optional. Staff are also offered the possibility to have the examination performed by a physician of their choice, and then get the expenses reimbursed (they are also informed of the practical steps they must take herefor). The staff member goes through laboratory tests (analysed on behalf of the processor by Aleris Medilab, who submits the results to the processor) followed by consultations and examination by a physician.

The processing operation is concluded by the processor sending to ECDC the 'Certificate of Health', which is stored in the medical section of the personal file, along with any other medical opinions submitted by the data subject.

The results of the laboratory analyses and the physician's report are given to the data subject directly by the processor. The processor sends to the controller invoices detailing the rendered services; the controller removes the details and forwards to ECDC's Financing/Accounting Section only the total cost of the services for payment of the processor.

C. Start of processing: This personal data processing operation began in April 2005 when the agency was established in Stockholm

Categories of personal data whose processing is prohibited, with exceptions, by Regulation 45/2001 may include data: concerning health

Data likely to present specific risks may include processing of data relating to health; intended to evaluate personal aspects relating to the data subject

Other categories of personal data may include data: in the form of personal identification numbers; concerning the physical characteristics of persons; concerning the data subject's family; concerning the data subject's career; concerning telephone numbers and communications

7/ Information to be given to data subjects

Detailed information is provided in a notice (attached herewith - Annex II) sent with the yearly reminder to staff by the controller.

8/ Procedures to grant rights of data subjects (*rights of access, to rectify, to block, to erase, to object*)

ACCESS (in accordance with Article 13 of Regulation (EC) 45/2001; and with Article 26(a) of the Staff Regulations, read in conjunction with Article 11 of the Conditions of Employment of Other Servants of the Communities): **Data held by the processor:** data subjects may request access to their medical and related administrative data from the processor directly, or indirectly from the controller who instructs the processor to grant the right. **Data held by the controller:** data subjects may request access to their medical and related administrative data from the controller directly. Regardless of the holder of the data, and depending on the wish of the data subject, access rights are granted by allowing on-the-spot inspection or by giving/sending the data subject electronic or paper copies, indeed within three months of receipt of the request by the controller and free of charge.

RECTIFICATION (in accordance with Article 14 of Regulation (EC) 45/2001): **Data held by the processor:** data subjects may request rectification of their medical and related administrative data from the processor directly, or indirectly from the controller who instructs the processor to grant the right. This includes adding counter-opinions by another doctor. **Data held by the controller:** data subjects may request rectification of their medical and related administrative data from the controller directly. This includes adding counter-opinions by another doctor. Regardless of the holder of the data, the request is granted without delay.

BLOCKING (in accordance with Article 15 of Regulation (EC) 45/2001), **ERASURE** (in accordance with Article 16 of Regulation (EC) 45/2001), **OBJECTION** (in accordance with Article 18 of Regulation (EC) 45/2001): **Data held by the processor:** data subjects may request the blocking or the erasure, or may object the processing, of their medical and related administrative data from the processor directly, or indirectly from the controller who instructs the processor to grant the right. **Data held by the controller:** data subjects may request the blocking or the erasure, or may object the processing, of their medical and related administrative data from the controller directly.

9/ Automated / Manual processing operation

Processing of data is automated (in electronic databases) and manual as part of a paper-based filing system.

10/ Storage media of data

Processor: data is stored electronically. Controller: the 'Certificate of Health' is stored in the individual personal files. Financial administrative data are stored manually and electronically.

11/ Legal basis and lawfulness of the processing operation

> Article 29(1) of Regulation (EC) 851/2004 (establishing ECDC), in conjunction with the first paragraph of Article 16 and with Article 91 of the Conditions of Employment of Other Servants of the Communities; Article 59(6) (by analogy) of the Staff Regulations of Officials of the Communities.

> Data subject's consent (for optional HIV testing)

12/ The recipients or categories of recipient to whom the data might be disclosed

> Staff under the direct authority of the controller: personnel administration team and secretariat of ECDC's Human Resources Section: 'Certificate of Health'; detailed invoices for services rendered by the processor

> Other ECDC staff: Finance Section: invoices showing the total cost of medical services by the processor;

> Processor, staff under processor's direct authority: Feelgood/Östermalmshälsan, Stockholm

> Processor on behalf of processor: Aleris Medialab AB, Stockholm

> Other EU institutions/bodies: Financial Identification and Legal Entity files of the data subject are inserted in the accounting system ABAC, which is accessible to all EU institutions/bodies. Data on the reimbursement of travel costs and on the payment of medical invoices are also inserted in ABAC, but are accessible only to a competent officer at the 'Treasury Management' unit in DG BUDG of the European Commission and only on specific request from ECDC's Accounting Officer for assistance in finding a solution to problems encountered whilst executing payment run and bank reconciliation procedures concerning payments under the Accounting Officer's competence.

This competent officer of 'Treasury Management' has provided ECDC with a relevant declaration of confidentiality (attached herewith - Annex III).

13/ retention policy of (categories of) personal data

The Certificate of Health and the laboratory/examination results are kept for a maximum of thirty years, in line with maximum limitation periods for private law claims (by virtue of Article 340 of the Treaty on the Functioning of the European Union in conjunction, e.g., with Section 199 of the German Civil Code). Related administrative financial data are kept for at least five years from the date on which the European Parliament grants discharge for the budgetary year to which the data relate (Article 49(d) of the Implementing Rules to the EU Financial Regulation); Legal Entity and Financial Identification files are kept as long as they are active in the financial system ABAC managed by the Commission.

13 a/ time limits for blocking and erasure of the different categories of data

(on justified legitimate request from the data subject)

(Please, specify the time limits for every category, if applicable)

Data are blocked / erased within reasonable time periods.

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,

Data are not processed for historical, statistical or scientific purposes.

15/ Proposed transfers of data to third countries or international organisations

Data are not transferred to non-EU countries or other international organisations.

16/ The processing operation presents specific risk which justifies prior checking (*please describe*):

This processing operation present specific risks because it involves data relating to health (medical examination, certificate of health, related administrative data) and is intended to evaluate personal aspects relating to the data subject, namely to determine whether the servant is fit for service.

AS FORESEEN IN:

Article 27.2.(a)

Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures,

Article 27.2.(b)

Processing operations intended to evaluate personal aspects relating to the data subject,

Article 27.2.(c)

Processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes,

Article 27.2.(d)

Processing operations for the purpose of excluding individuals from a right, benefit or contract,

Other (general concept in Article 27.1)

17/ Comments

All ECDC staff members have been informed about confidentiality in processing personal data and received instructions by the Data Protection Officer. The agency is in the process of carrying out training/information sessions.

INFORMATION TO BE GIVEN⁽²⁾

(2) Please attach all necessary backup documents

1/ Name and address of the controller

Jessica Mannheim, Head of Human Resources Section; ECDC, SE-17183 Stockholm,
jessica.mannheim@ecdc.europa.eu

2/ Organisational parts of the institution or body entrusted with the processing of personal data

- > ECDC Administration Unit, Human Resources Section (as 'controller');
- > Feelgood Östermalmshälsan AB (Box 27301, SE-10254 Stockholm; corporate identity number 556185-6385 - as 'processor');
- > Aleris Medilab (Stockholm; corporate identity number 556052-8746 - as 'processor' for the processor).

3/ Name of the processing

Pre-recruitment medical examination

4/ Purpose or purposes of the processing

To determine whether an incoming ECDC servant is physically fit to perform his/her prospective duties.

5/ Description of the category or categories of data subjects

Incoming ECDC Temporary Staff and Contract Staff

The data are collected from the data subjects themselves.

6/ Description of the data or categories of data *including, if applicable, special categories of data (article 10) and/or origin of data*

A. Data categories

1. **Laboratory analyses:** blood analysis, consisting in biochemical, lipids, red blood cells, white blood cells, serology (Hepatitis B/C, optionally HIV); urinalysis; hearing test; electrocardiogram; spirometry.
2. **'Medical Examination' report** (template attached herewith)
3. **'Medical Examination Before Appointment'** (template attached herewith): family medical history, personal medical history.
4. **'Certificate of Health'** (template attached herewith), stating whether the data subject is 'in good health and fit for work, both mentally and physically'.
5. **Data subject identification** data (name, age, date of birth, personal identification number).
6. **Related administrative data** such as medical appointments, travel/accommodation.

B. Description of personal data processing operation

Persons to whom, on condition of passing a medical examination, the ECDC has offered an employment contract (the 'data subjects'), make, at the request of the controller (ECDC's Human Resources Section), an appointment with, and visit, the processor (Feelgood Östermalmshälsan AB), who examines them medically on behalf of ECDC. In particular, data subjects fill out and hand to medical personnel

(nurses, physicians) of the processor a questionnaire entitled 'Medical Examination Before Appointment', currently also used by the European Commission (no other party annotates this questionnaire in any way). The medical personnel then physically examine, and take samples from, the data subjects (optionally, a separate sample is taken, or a test on other samples is carried out, for establishing whether a data subject is HIV positive - a nurse informs the data subject of this possibility, and ask for its written consent expressly on a purely voluntary basis). The samples are analysed on behalf of the processor by Aleris Medilab, who submits the results to the processor.

The processing operation is concluded by the processor sending to ECDC the 'Certificate of Health' and, in a sealed envelope, a) the 'Medical Examination Before Appointment', b) the laboratory results and c) the 'Medical Examination' report. The sealed envelope is handed by the controller to the data subject, who signs to acknowledge receipt. The 'Certificate of Health' is stored in the medical section of the personal file, along with any other medical opinions submitted by the data subject.

If the data subject needs to travel to the place of establishment of the processor, ECDC Missions, Meetings and Logistics Section, process such relevant data as transport tickets, accommodation, invoices and financial details of the data subject (the latter in the form of 'Financial Identification' and 'Legal Entities' forms used by every EU institution/body). The processor sends to the controller invoices, detailing the rendered services; the controller forwards to ECDC's Financing/Accounting Section only the total cost of the services for payment of the processor and financial details.

C. Start of processing: This personal data processing operation began in April 2005 when the agency was established in Stockholm.

Categories of personal data whose processing is prohibited, with exceptions, by Regulation 45/2001 include data concerning health.

Data likely to present specific risks may include data processing of data relating to health; intended to evaluate personal aspects relating to the data subject; processing operations for the purpose of excluding individuals from a contract.

Other categories of personal data may include data in the form of personal identification numbers; concerning the physical characteristics of persons; concerning bank accounts; concerning recruitment; concerning the data subject's family; concerning the data subject's career; concerning telephone numbers and communications.

7/ Information to be given to data subjects

1. Data subjects are provided with the information contained in the 'Medical Examination Before Appointment'.
2. More detailed information is attached as a notice (attached herewith) to the invitation to staff by the controller to perform the examination.

8/ Procedures to grant rights of data subjects (*rights of access, to rectify, to block, to erase, to object*)

ACCESS (in accordance with Article 13 of Regulation (EC) 45/2001; and with Article 26(a) of the Staff Regulations, read in conjunction with Article 11 of the Conditions of Employment of Other Servants of the Communities): **Data held by the processor**: data subjects may request access to their medical and related administrative data from the processor directly, or indirectly from the controller who instructs the processor to grant the right. **Data held by the controller**: data subjects may request access to their medical and related administrative data from the controller directly. Regardless of the holder of the data, and depending on the wish of the data subject, access rights are granted by allowing on-the-spot inspection or by giving/sending the data subject electronic or paper copies, indeed within three months of receipt of the request by the controller and free of charge.

RECTIFICATION (in accordance with Article 14 of Regulation (EC) 45/2001): **Data held by the processor**: data subjects may request rectification of their medical and related administrative data from the processor directly, or indirectly from the controller who instructs the processor to grant the right. This includes adding counter-opinions by another doctor. **Data held by the controller**: data subjects may request rectification of their medical and related administrative data from the controller directly. This includes adding counter-opinions by another doctor. Regardless of the holder of the data, the request is granted without delay.

BLOCKING (in accordance with Article 15 of Regulation (EC) 45/2001), **ERASURE** (in accordance with Article 16 of Regulation (EC) 45/2001), **OBJECTION** (in accordance with Article 18 of Regulation (EC) 45/2001): **Data held by the processor**: data subjects may request the blocking or the erasure, or may object the processing, of their medical and related administrative data from the processor directly, or indirectly from the controller who instructs the processor to grant the right. **Data held by the controller**: data subjects may request the blocking or the erasure, or may object the processing, of their medical and related administrative data from the controller directly.

9/ Automated / Manual processing operation

Processing of data is automated (in electronic databases) and manual as part of a paper-based filing system.

10/ Storage media of data

Processor: data is stored electronically. Controller: (administrative) data is stored in individual personal files.

11/ Legal basis and lawfulness of the processing operation

- > Article 29(1) of Regulation (EC) No 851/2004 (establishing ECDC), in conjunction with
 - > (for determining whether an incoming servant is fit for service:) Articles 12(2)(d) and 13 (for Temporary Staff) and Articles 82(3)(d) and 83 (for Contract Staff) of the Conditions of Employment of Other Servants of the Communities; Article 33 (by analogy) of the Staff Regulations of Officials of the Communities
 - > (for excluding servants from the reimbursement of sickness expenditure:) Article 28 (for Temporary Staff) and Article 95 (for Contract Staff) of the Conditions of Employment of Other Servants of the Communities
 - > (for deferring benefits regarding invalidity or death:) Article 32 (for Temporary Staff) and Article 100 (for Contract Staff) of the Conditions of Employment of Other Servants of the Communities
- > Data subject's consent (for optional HIV testing)

12/ The recipients or categories of recipient to whom the data might be disclosed

> Staff under the direct authority of the controller: personnel administration team, secretariat (the 'Certificate of Health' and, in a sealed envelope, a) the 'Medical Examination Before Appointment', b) the laboratory results and c) the 'Medical Examination' report); invoices for detailed rendered services
> Other ECDC staff:

Mission Meetings Logistic Section: Travel tickets and hotel bookings, plus related invoices

Finance Section: invoices for travel/accomodation; invoices showing the total cost of medical services by the processor; Legal Entity and Financial Identification files

> Processor, staff under processor's direct authority: Feelgood/Östermalmshälsan, Stockholm

> Processor on behalf of processor: Aleris Medialab AB, Stockholm

> Other EU institutions/bodies: Financial Identification and Legal Entity files of the data subject are inserted in the accounting system ABAC, which is accessible to all EU institutions/bodies. Data on the reimbursement of travel costs and on the payment of medical invoices are also inserted in ABAC, but are accessible only to a competent officer at the 'Treasury Management' unit in DG BUDG of the European Commission and only on specific request from ECDC's Accounting Officer for assistance in finding a solution to problems encountered whilst executing payment run and bank reconciliation procedures concerning payments under the Accounting Officer's competence. This competent officer of 'Treasury Management' has provided ECDC with a relevant declaration of confidentiality (copy attached herewith).

13/ retention policy of (categories of) personal data

The medical statement/certificate, the medical questionnaire, and the laboratory results on both recruited and non-recruited candidates are kept for a maximum of thirty years, in line with maximum limitation periods for private law claims (by virtue of Article 340 of the Treaty on the Functioning of the European Union in conjunction, e.g., with Section 199 of the German Civil Code). Related administrative financial data are kept for at least five years from the date on which the European Parliament grants discharge for the budgetary year to which the data relate (Article 49(d) of the Implementing Rules to the EU Financial Regulation); Legal Entity and Financial Identification files are kept as long as they are active in the financial system ABAC managed by the Commission.

13 a/ time limits for blocking and erasure of the different categories of data (on justified legitimate request from the data subject)

(Please, specify the time limits for every category, if applicable)

Data are blocked / erased within reasonable time periods.

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,

Data are not processed for historical, statistical or scientific purposes.

15/ Proposed transfers of data to third countries or international organisations

Data are not transferred to non-EU countries or other international organisations.

16/ The processing operation presents specific risk which justifies prior checking (please describe):

This processing operation present specific risks because it involves data relating to health (medical examination, medical certificate, related administrative data) and is intended to evaluate personal aspects relating to the data subject, namely to determine whether the incoming servant is fit for service.

AS FORESEEN IN:

Article 27.2.(a)

Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures,

Article 27.2.(b)

Processing operations intended to evaluate personal aspects relating to the data subject,

Article 27.2.(c)

Processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes,

Article 27.2.(d)

Processing operations for the purpose of excluding individuals from a right, benefit or contract,

Other (general concept in Article 27.1)

17/ Comments

All ECDC staff members have been informed about **confidentiality** in processing personal data and received instructions by the Data Protection Officer. The agency is in the process of carrying out training/information sessions.

PLACE AND DATE: Stockholm (Sweden), 29/01/2010

DATA PROTECTION OFFICER: Elisabeth Robino

SIGNATURE:

INSTITUTION OR BODY: European Centre for Disease Prevention and Control (ECDC)