Data protection statement on the processing of personal data in the context of staff requests that require medical assessments by the EPO Occupational Health Services (OHS)

Protecting your privacy is of the utmost importance to the European Patent Office (EPO). We are committed to protecting your personal data and ensuring respect for data subjects' rights when performing our tasks and providing our services. All data of a personal nature that identify you directly or indirectly will be processed lawfully, fairly and with due care.

The processing operations described below are subject to the EPO Data Protection Rules (DPR).

The information in this statement is provided in accordance with Articles 16 and 17 DPR.

This statement relates to the medical assessments carried out by the EPO OHS at the request of staff and in the cases provided for by the Service Regulations.

1. What is the nature and purpose of the processing operation?

This data protection statement relates to the processing of personal and medical data for the following purposes:

- To process staff requests for granting benefits or settling disputes as provided for in the Service Regulations
- To improve the wellbeing of staff and their families

The EPO OHS department is made up of medical and administrative staff.

The medical staff provide medical assessments in the following cases:

a. Assessment of dependants' disabilities or serious illness for the granting of special allowances and reimbursement
Staff members can use a MyFIPS online form to request an assessment of the medical conditions of their dependants with a view to being granted the allowances under Article 69(5)(8) and the reimbursements under Article 69(10) ServRegs. The request is received by OHS staff and stored in the EPO medical database (Cority).
The conclusion of the medical assessment (which does not contain any medical information) is sent to the requester and HR salary department for registration of the relevant information in FIPS and for payment purposes.
If the request is sent via the HR ticketing system, the HR interlocutors will have access to the administrative information of the request but not to any medical information.
Outlook may also be used for sharing information between OHS and the requester. If OHS has to share any confidential medical information with the requester, the file containing such information will be encrypted or password protected.

b. Assessment of family member's illness for the granting of special and family leave
Staff members submit their requests to the HR interlocutors via the HR ticketing system and send the required medical information to OHS by email.
Any medical information is stored by OHS in the medical database.
The conclusion of the medical assessment (which does not contain any medical information) is sent to the HR interlocutors by email for registration of the relevant information in FIPS. HR interlocutors will also inform the

requester and their line manager regarding the conclusions of the medical assessment (which does not contain any medical information).

c. Settlement of disputes between staff and the health insurance administrator (Cigna) on reimbursement of medical expenses
Staff members normally send their request to OHS via MyFIPS online form or email. The medical information provided is stored by OHS in the medical database.
Information for the settlement of the disputes between Cigna and OHS may be exchanged by email and is encrypted via TSL (transport layer security). The conclusion of the medical assessment is sent to the requester and Cigna by email and, in principle, does not contain medical information.
In some specific cases and to prevent any reimbursement disputes, Cigna may ask OHS for advice on the eligibility of a medical treatment for reimbursement. In these cases, the medical documents are, in principle, anonymised.

d. Granting of sick leave for spa cures
The request for a spa cure (type A or B) is sent by the staff member to OHS via MyFIPS online form.
Family members and pensioners send requests for type A cures to OHS by email. The request contains a medical prescription and report. The medical assessment of OHS medical staff on the granting of sick leave is based on this document.
The assessment is sent by email to the HR Interlocutors for registration of the sick leave in the HR database (SAP FIPS), to the line manager and also to Cigna for type A cures. This assessment does not contain any medical information.
Email communication between Cigna and OHS is encrypted via TSL (transport layer security).
Family members and pensioners send requests for type B cures per email to Cigna directly.

In all the cases mentioned above:
• no medical information is exchanged between OHS staff and the management, the HRBP and HR interlocutors.
• any medical information (e.g. date of the consultation, medical notes, medical reports) is stored in the EPO medical database (Cority).

Data subjects are
• employees
• pensioners (cases a, c and d)
• externals (employees' and pensioners' family members (case d), widows, heirs (cases a, c and d), treating physicians of the requester)

The processing is not intended to be used for any automated decision-making, including profiling.

Your personal data will not be transferred to recipients outside the EPO which are not covered by Article 8(1), (2) and (5) DPR unless an adequate level of protection is ensured. In the absence of an adequate level of protection, a transfer can only take place if appropriate safeguards have been put in place and enforceable data subject rights and effective legal remedies for data subjects are available, or if derogations for specific situations as per Article 10 DPR apply.

2. What personal data do we process?

In all above-mentioned procedures, the following categories of personal data of employees, pensioners and their family members may be processed:

Surname, first name, gender, personnel number, date and place of birth, nationality, civil status, children's name and date of birth, languages, postal addresses, email address, telephone numbers, room number, name, contact details of the treating physician, job profile, type of contract, line manager name, type and duration of

absences from work, date/time of medical consultations, sickness statistics, sick leave certificates, medical opinions (always issued without medical data).

In all above-mentioned procedures, the following special categories of personal data may be processed:

Medical data: personal medical history, medical reports provided by the employee, medical reports provided by EPO specialists after consultation with the employee, medical notes recorded after a consultation, medical certificates and diagnoses.

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of Directorate 423 Essential Services, acting as the EPO's delegated data controller.

Personal data are processed by the EPO staff of D 4234 Occupational Health Services involved in managing the activity referred to in this statement.

External contractors involved in maintaining certain services may also process personal data, which may include accessing them.

4. Who has access to your personal data and to whom are they disclosed?

The following recipients may have access to the categories of personal data (excluding medical data) mentioned above on a need-to-know basis only:

• HR interlocutors. In particular, they may receive the request (in cases a and b) and process it once they receive the medical conclusion (case b).
• Line manager is informed by HR interlocutors when case b requests are granted and by OHS when case d requests are granted.
• Legal Services may have access to personal data for the prevention and management of grievances.
• Directorate Ethics and Compliance (DEC) may have access to personal data within the framework of their investigative mandate.
• SAP Centre of Excellence department. A very limited number of staff in this department provides technical support to maintain the medical database (Cority), in particular for system configuration purposes (i.e. creation, update and deletion of general system settings including language; screen layouts including the configuration of fields displayed on screens; look-up tables; business rules including field input checks; roles and profiles) and user management (i.e. creation and deletion of user accounts and the assignment of roles)
• Microsoft Office
• SAP FIPS

The following recipients may also have access to the medical data mentioned above on a need-to-know basis only:

• Treating physician of an employee when the employee has expressly authorised EPO medical staff to exchange information with their treating physician (under Article 89(3) ServRegs).
• Health insurance administrator (Cigna) in the framework of processing cure requests, disputes on medical reimbursements, detecting health care frauds.
• SAP Centre of Excellence department. Only one employee in this department with the role of system configurator is allowed full access to medical data. This is necessary to ensure the functionality and efficiency of the application.

Personal data may be disclosed to third-party service providers for maintenance and support purposes.

Personal data may be disclosed on a need-to-know basis to staff member(s) of the unit(s) involved in the prevention and settlement of legal disputes (whether in internal, judicial or alternative redress mechanisms afforded by the EPO or any other legal processes involving the EPO) when this is necessary and proportional for them to perform tasks carried out in the exercise of their official activities, including representing the EPO

in litigation and pre-litigation. Such processing will take place on a case-by-case basis in accordance with the DPR requirements and with the principles of confidentiality and accountability.

Personal data will only be shared with authorised persons responsible for the necessary processing operations. They will not be used for any other purposes or disclosed to any other recipients.

5. How do we protect and safeguard your personal data?

We take appropriate technical and organisational measures to safeguard and protect your personal data from accidental or unlawful destruction, loss or alteration and unauthorised disclosure or access.

All personal data are stored in secure IT applications in accordance with the EPO's security standards. Appropriate levels of access are granted individually only to the above-mentioned recipients.

For systems hosted on EPO premises, the following base security measures generally apply:

- user authentication and access control (e.g. role-based access control to the systems and network, principles of need-to-know and least privilege);
- logical security hardening of systems, equipment and network;
- physical protection: EPO access controls, additional access controls to datacentre, policies on locking offices;
- transmission and input controls (e.g. audit logging, systems and network monitoring);
- security incident response: 24/7 monitoring for incidents, on-call security expert.

In principle, the EPO has adopted a paperless policy management system; however, if paper files containing personal data need to be stored on EPO premises, they are locked in a secure location with restricted access. When data are outsourced (e.g. stored, accessed and processed), a privacy and security risk assessment is carried out.

For personal data processed on systems not hosted on EPO premises, the providers processing the personal data have committed in a binding agreement to comply with their data protection obligations under the applicable data protection legal frameworks. The EPO has also carried out a privacy and security risk assessment. These systems are required to have implemented appropriate technical and organisational measures, such as physical security measures; access and storage control measures; securing data at rest (e.g. by encryption); user, transmission and input control measures (e.g. network firewalls, network intrusion detection system (IDS), network intrusion protection system (IPS), audit logging); conveyance control measures (e.g. securing data in transit by encryption).

6. How can you access, rectify and receive your data, request that your data be erased, or restrict/object to processing? Can your rights be restricted?

Data subjects have the right to access, rectify and receive their personal data, not to be subject to a decision based solely on automated processing, to have their data erased and to restrict and/or object to the processing of their data (Articles 18 to 24 DPR). Their right to rectification applies only to factual and objective data processed as part of the medical procedure. It does not apply to subjective statements (which, by definition, cannot be factually wrong).

Data subjects are also entitled to withdraw consent given in the past at any time with effect for the future (N.B. the withdrawal of consent does not affect the lawfulness of the processing based on the consent prior to the withdrawal).

If you have any questions about the processing of your personal data that does not require access to your medical data, please write to the delegated data controller at pdpeople-dpl@epo.org. For any other data

subject request that requires access to your medical data, please write to the medical services at healthandsafety@epo.org. In order to enable us to respond more promptly and precisely, you always need to provide certain preliminary information with your request. We therefore encourage you to fill in this form (for internals), this form (for externals) or this form (for pensioners) and submit it with your request.

We will reply to your request without undue delay and in any event within one month of receipt of the request. However, Article 15(2) DPR provides that this period may be extended by two further months where necessary in view of the complexity and number of requests received. We will inform you of any such delay.

Data subject rights might be restricted in the following cases:

• On a case-by-case basis, the EPO may restrict the data subject's right to access their personal medical data and/or files in its possession, in particular where the exercise of that right would adversely affect the rights and freedoms of the data subject or other data subjects (Article 4(1)(d) of Circular No. 420 implementing Article 25 DPR).
• If the medical data and/or file refers to an employee affected by severe psychiatric and psychological problems and access to such data is likely to represent a risk to the employee's health (e.g. in the case of a documented suicide risk), access may be restricted by the EPO. In these cases, access to such information will be given to a doctor of the employee's choice (Article 8 of Circular No. 420 implementing Article 25 DPR).
• In exceptional cases where the employee has a severe mental illness that prevents them from taking care of themselves and puts them and/or others at serious risk and any other remedies have been exhausted, the EPO OHS may involve the national social/security services to protect the rights and health of staff and/or others (Article 4(1)(d) of Circular No. 420 implementing Article 25 DPR).

7. What is the legal basis for processing your data?

Personal data are processed on the basis of Article 5(a) DPR in conjunction with:
Article 11(2)(b) DPR: "Processing of special categories of personal data ("processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security law insofar as it is authorised by legal provisions of the European Patent Organisation providing for appropriate safeguards for the fundamental rights and the interests of the data subject" and
Article 11(3) DPR: Processing of special categories of data "... is required for the purposes of preventive or occupational medicine, the assessment of an employee's working capacity, medical diagnosis, the provision of health or social care or treatment, the management of health or social care systems and services or medical examinations and opinions provided for in the Service Regulations or other legal provisions of the European Patent Organisation and where those data are processed by a health professional subject to the obligation of professional secrecy or by another person subject to an equivalent obligation of secrecy."

Article 5(d) DPR applies if the employee is asked to consent to the exchange of medical information between their treating physician / an EPO medical expert and the EPO medical practitioner. This may happen when the EPO medical practitioner has to assess the employee's medical condition in the framework of the processing operations in hand.
Consent must be freely given, specific, informed, unambiguous and affirmative. The employee is free to refuse or withdraw their consent without any detriment at any time, in which the relevant medical assessment will be done on the basis of the information available.

Legal references for the different services.

a. Assessment of dependants' disabilities or serious illness for the granting of special allowances and reimbursement
Articles 69(5),(8) and (10) and 89-90 ServRegs

b. Assessment of family member's illness for the granting of special and family leave

Article 45b(1) ServRegs; Circular No. 22, Rule 3; Article 45b(c)(ii) and (iii) ServRegs; Article 59(3) ServRegs; Circular No. 22, Rule 8 (Article 59 ServRegs)

c. Settlement of disputes between staff and the health insurance administrator (Cigna) on reimbursement of medical expenses
Circular No. 236, Circular No. 178, Articles 89-90 ServRegs

d. Granting of sick leave for spa cures
Article 83 ServRegs; Circular No. 367, Article 1D (Sick leave in case of spa cures); Circular No. 368 – Guide to cover.

Any exchange of medical information between the EPO medical practitioner and any external doctor will be done without prejudice to any applicable deontological national rule.

The EPO's OHS and the relevant procedures are undergoing a reorganisation that should be finalised by 2023. The operational guidelines and the legal framework will be revised and updated accordingly.

8. How long do we keep your data?

Cority has served as the main medical database since 2006. As of 2016, data are stored electronically only in the EPO medical database.

Currently, the data is permanently kept in the electronic database due to technical constraints.

However, by 2024, the following retention periods should be implemented:

a. Assessment of dependants' disabilities or serious illness for the granting of special allowances and reimbursement – five years as of the end date of the allowance.
b. Assessment of family member's illness for the granting of special and family leave – five years as of the case closure date.
c. Settlement of disputes between staff and the health insurance administrator (Cigna) on reimbursement of medical expenses – ten years as of the case closure date.
d. Granting sick leave for spa cures – ten years as of the case closure date.

The retention periods apply unless litigation is pending. In case of pending litigation, the retention period will be suspended until all means of redress have been exhausted or the decision is final.

All data stored in the common Outlook inboxes and calendars of OHS which are older than five years are deleted.

No retention period currently applies to personal data stored in SAP FIPS.

SAP MyFIPS is used by employees to send cure requests, which are encryption protected. The encrypted data are automatically deleted from the server after 90 days and from the PC of administrative staff on confirmation that the data have been uploaded to Cority or on closing the encryption application (MedXfer).

In principle, all data are stored electronically only. However, some old medical paper files are still stored in secured locked rooms, only accessible to authorised staff, which should be deleted by 2024.

9. Contact information

If you have any questions about the processing of your personal data, please write to the delegated data controller at pdpeople-dpl@epo.org. If you are an external data subject, please write to *DPOexternalusers@epo.org*.

You can also contact our Data Protection Officer at dpo@epo.org (for internals)/ *DPOexternalusers@epo.org* (for externals).

Review and legal redress

If you consider that the processing infringes your rights as a data subject, you have the right to request review by the controller under Article 49 DPR and, if you disagree with the outcome of the review, the right to seek legal redress under Article 50 DPR.