Data protection statement on the processing of personal data within the framework of the Employee Assistance Programme (EAP)

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.

The EPO has assigned the following tasks to external providers (hereinafter "Contractors"):

(1) Providing staff members and their dependants with free access to psychosocial support and counselling if there is a need to help reconcile work and home life,
(2) Providing an online platform that includes information about health and wellbeing.

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

This data protection statement relates to the processing of personal data for the provision and administration of the Employee Assistance Programme (EAP).

Staff members and dependants may contact the EAP Care Access Centre for confidential short-term counselling to solve personal or work-related problems, pressures and stress situations.
In particular, assistance is provided for:

- Coping with isolation and loneliness
- Adapting across cultures
- Identifying and coping with culture shock
- Addressing the personal impact of the relocation
- Dealing with stress, anxiety and depression
- Addressing alcohol and drug misuse
- Resolving marital and relationship difficulties
- Finding solutions for work-related issues
- Offering advice and referrals for work-life issues such as family support / parenting / elder care
- Accessing crisis and trauma support
- Addressing legal or financial issues
- Working towards life goals
- Strengthening relationships
- Improving communication.

The procedure can be described as follows.

- The first contact is made by phone.
- Staff members/dependants have to state the name of the EPO to identify the employer offering this service.
- They are free to remain anonymous by using a pseudonym.
- Email address and / or phone number are needed by the provider as contact data.
- Other personal data and information may be required, depending on the support provided. These additional personal data are always taken for the purpose of providing the specific support requested.
- After a preliminary case assessment, the EAP Care Access Centre identifies a specialist with whom the staff member/dependant can have approximately six support sessions over the telephone, online or in person.

- If the staff member/dependant needs more specialised or long-term support, the service provider helps them select an appropriate specialist or service.
- Once a case is closed, the staff member/dependant is asked by the provider to evaluate the service via an anonymous survey.
- The D4234 Occupational Health Services receive aggregated data reports from the service provider quarterly and annually.
- In addition, the EAP offers an online platform that can be accessed via an app or PC. EPO work credentials rather than individual ones are used to access this platform.
- The platform provides information about health and wellbeing and offers the possibility to contact the EAP Care Access Centre.

AWP Health & Life Services Limited (Allianz) and Telus Health (formerly LifeWorks and LifeWorks was formerly Morneau Shepell) are responsible for processing the personal data provided directly by users of the services.

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?

The following categories of personal data are processed for internals:
- Contact data: home address, personal email, phone numbers
- Sensitive data: health data
- Employment data: company entity

The following categories of personal data are processed for externals:
- Contact data: home address, personal email, phone numbers
- Sensitive data: health data
- Employment data: company entity

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of D423 HR Essential Services, acting as the EPO's delegated data controller.

External contractors involved in carrying out the Employee Assistance Programme (EAP) may also process personal data, which may include accessing them.

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.

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

Within the EPO, only aggregated data or the anonymous surveys are shared with D 4.2.3, D 4.2.2, PD 4.2, the Vice-President DG 4, the President and the COHSEC.

Outside the EPO, Telus Health handles all processing of personal data and is the only party with access to raw personal data.

Information relating to participation in the EAP is strictly confidential. No information is shared with anyone without informed, voluntary and written consent. Only in order to protect the vital interest of the staff/dependant

or third parties, may, and indeed must, the external service provider inform the national authorities and disclose personal data.

Allianz only receives the same data as the EPO, in other words, the results of aggregated, anonymised reports of service satisfaction and the "Utilisation report".

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

Personal data may be disclosed on a need-to-know basis to the 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 a 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?

Users 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 object to the processing of their data (Articles 18 to 24 DPR).

If you would like to exercise any of these rights, external users should write to DPOexternalusers@epo.org, otherwise contact the delegated data controller at pdpeople-dpl@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 externals) or this form (for internals) 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.

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

Personal data are processed on the basis of Article 5a DPR (processing is necessary for the EPO's management and functioning).

8. How long do we keep your data?

Personal data will be kept only for the time needed to achieve the purposes for which they are processed.

In the event of a formal appeal/litigation, all data held at the time the formal appeal/litigation was initiated will be retained until the proceedings have been closed.

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 external, please write to DPOexternalusers@epo.org.

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.