Data protection statement on the processing of personal data for mass email distribution list management

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 record of processing activity relates to the mass email distribution list management *w*hich is performed with the SendInBlue tool. This tool is used for the dispatch of mass e-mails, covering the automated collection, use, storage, transfer and destruction of email addresses and site information used to target specific subparts of the organisation or external users, as well as the manual addition of new records and the manual deletion of departing members.

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

This data protection statement relates to the processing of personal data within the context of mass email distribution list management with the Sendinblue tool.

More specifically, the main use case relates to mass emails addressed internally to EPO colleagues, such as for example mass e-mails from Amicale, staff representation etc. Based on approved business cases (for example site-specific mails), the sending area will use their associated authorised email address (shared mailboxes owned by the relevant area) to send their mass mail to the tool, which will first check that the sender is indeed authorised and then forward the mail to the associated distribution list. The distribution lists are associated per authorised sending email address. The tool automatically tracks the opt out. BIT is responsible for the implementation, setup and maintenance of the environment for sending the mass mails and the distribution lists for the above are periodically (generally twice a month) extracted from the EPO Phone book and uploaded to the SendInBlue tool by BIT. Recipients can unsubscribe by opting-out from these distribution lists.

A second use case relates to mass emails addressed by specific business areas of the Office to mailing lists including externals (e.g. Patent Academy). In these cases, the business area would have to periodically provide an up-to-date distribution list to BIT for uploading into the tool, as this cannot be derived from the phone book. The specific business areas will also remain responsible for confirming the opt-in (consent) of recipients. The consent management, if any is necessary, is handled by the respective business unit.

For both use cases the units sending the emails remain responsible for the contents of their messages, including responsibility for any personal data potentially included in their messages.

Therefore, as outlined, personal data are processed for the managing mass e-mail distribution lists.

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 **Employees and Contractors**:
- User Account Information: User ID
- Browsing Information: IP Address
- Personal Identification: Full Name
- Correspondence: Personal Information Provided Voluntarily
- Employment Information: Company Entity, Office Location
- Contact Information: Working E-Mail Address, Contact Details, Country, Home Address, Phone Numbers

The following categories of personal data are processed for **Externals**:
- Browsing Information: IP Address
- Contact Information: Working E-Mail Address, Phone Numbers
- Personal Identification: Full Name

3. Who is responsible for processing the data?

Personal data are processed under the responsibility of EPO Principal Directorate CIO, acting as the EPO's delegated data controller.

External contractors involved in providing services may also process personal data, which can include accessing it.

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

Personal data are disclosed on a need-to-know basis to the EPO staff working in BIT for the purpose of managing the service.

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

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 basic 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.

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 assessed and verified the technical and organisational measures within the binding agreement. 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?

You have the right to access, rectify and receive your personal data, not to be subject to a decision based solely on automated processing, to have your data erased and to restrict and/or object to the processing of your data (Articles 18 to 24 DPR).

If you would like to exercise any of these rights, external users should write to the delegated data controller at DPOexternalusers@epo.org, otherwise internals should contact the delegated controller at DP_BIT@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), 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 5 (a) of the DPR i.e. processing is necessary for the performance of a task carried out in the exercise of the official activities of the European Patent Organisation or in the legitimate exercise of the official authority vested in the controller, which includes the processing necessary for the Office'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 it is processed. Data will be deleted upon departure of the staff member for EPO staff, young professionals and seconded national experts. Personal data of externals, including members of the general public, who opt into a list and do not opt out, will be deleted upon decommissioning of the distribution list. Personal data of externals who have opted out will be deleted when an up-to-date distribution list is periodically provided by the relevant business area.

At the end of the contractual relationship, Sendinblue undertakes to destroy all personal data within a maximum period of three (3) months, subject to Sendinblue's requirements to store data for legal purposes.

9. Contact information

External data subjects who have any questions about the processing of their personal data, should write to the delegated data controller and/or our Data Protection Officer at DPOexternalusers@epo.org.

EPO employees should contact the delegated data controller at DP_BIT@epo.org. Internals may also contact the Data Protection Officer at dpo@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.