

# Privacy Statement

This is a statement on the processing of your personal data pursuant to the EU's General Data Protection Regulation (2016/679) (GDPR).

## Controller

Motmedel AB

## Communication Regarding Privacy Matters

Email address: *dpo@motmedel.io*

We request that data subjects contact the person listed hereinabove for all questions related to the processing of personal data and situations related to the exercising of your rights.

## Basis and Purpose of Processing Personal Data

The legal basis for the processing of personal data

The controller's legitimate interest is based on securing companies and people by offering services that protect against cyber threats and data breaches. We have conducted a legitimate interest assessment and determined that our interest in processing this data to help users protect themselves outweighs the potential impact on individuals' rights and freedoms, especially since we take care to minimize data usage and protect privacy throughout the process.

Source of the data and exemption from notification

The personal data we process is sourced from publicly available data breach databases on the internet, without the direct knowledge or consent of the individuals involved. In accordance with Article 14(5)(b) of the GDPR, we are exempt from directly notifying these individuals, as doing so would involve disproportionate effort given the nature and scale of the data. Instead, we provide this information publicly through our privacy policy to ensure transparency.

The purpose of processing personal data

The purpose of processing personal data is to secure companies and people by offering services that protect against cyber threats.

## **Personal Data Being Processed**

The controller only collects personal data concerning the data subjects that are essential and relevant for the purposes explained in this privacy statement.

The following data concerning the data subjects are processed:

Personal data provided by users of our cybersecurity services:

- Contact information (such as names, email addresses, or phone numbers) and other identifiers (such as usernames or account details) that users provide to engage with our services, including for communication, account management, or service delivery.
- Data subjects: Individuals or representatives of companies who use our cybersecurity services to protect against cyber threats and data breaches.

Personal data sourced from publicly available data breach databases:

- Personal information that may include email addresses, usernames, passwords, names, phone numbers, addresses, or other personal data exposed in publicly available data breaches, which we use to provide services that help users identify and mitigate risks from such breaches.
- Data subjects: Individuals whose personal data has been exposed in publicly available data breaches, which may include both adults and children under the age of 18.

## **Retention Period for Personal Data**

The controller will process the personal data for as long as it is necessary to fulfill the purposes outlined in this privacy statement. The personal data will be deleted or anonymized once we determine that the service or customer relationship is no longer needed, unless we are required to retain the data longer to comply with legal obligations or regulatory requirements.

At the end of this period, the controller will delete or anonymize the data in accordance with the deletion processes it follows.

The controller may be obliged to process some personal data belonging to the filing system for longer than stated above to comply with the legislation or authority requirements.

## **Rights of the Data Subject**

**Right to Request Access to Personal Data**

The data subject has the right to receive confirmation regarding whether personal data concerning them is being processed and, if it is, the right to receive a copy of their personal data.

### **Right to Rectification**

The data subject has the right to request that inaccurate and erroneous personal data concerning them be rectified. The data subject also has the right to supplement incomplete personal data by submitting the required additional information.

### **Right to Erasure**

The data subject has the right to request the erasure of their personal data. This applies, for example, when the personal data is no longer needed for the purpose for which it was collected, when the personal data has been processed unlawfully, or if the data subject withdraws the consent on which the processing is based.

### **Right to Restriction of Processing**

The data subject has the right to request the restriction of processing of their personal data if, for example, the data subject objects to the correctness of the data or believes that the processing is against the law.

### **Right to Transfer Data (Data Portability)**

The data subject has the right to obtain the personal data relating to them and the personal data that the data subject themselves has submitted. The personal data must be disclosed in a structured, commonly used, and machine-readable format. The data subject also has the right to transfer this data to another controller.

### **Right to Lodge a Complaint with a Supervisory Authority**

The Swedish Authority for Privacy Protection is the national supervisory authority for personal data matters. The data subject have the right to bring your case to the supervisory authority if you consider that the processing of personal data concerning you is in violation of applicable law.

## **Information Relating to Children**

Within the framework of this policy, our service does not target children or actively collect their personal information. However, we acknowledge that the publicly available data breach databases we process, which are sourced from the

internet without the direct knowledge of the individuals involved, may contain personal information relating to children under the age of 18. In accordance with Article 14(5)(b) of the GDPR, we are exempt from directly notifying these individuals, including children or their guardians, as doing so would involve disproportionate effort. We take steps to minimize the use of such data and do not disclose any specific details from these databases, ensuring that our service prioritizes the privacy and protection of all individuals, including children.