Privacy Policy for the use of the PVRADAR App and website www.pvradar.com

Introduction

This Privacy Policy informs you about the type, scope and purpose of the collection and use of personal data when using the PVRADAR app (hereinafter referred to as '**App**') and the PVRADAR website www.pvradar.com (hereinafter referred to as "**website**"). For each data processing activity, we indicate whether it relates to the app and/or the website. The App/website is provided by Virtuous-Re GmbH (hereinafter referred to as '**Operator**'). The Operator is responsible for all personal data collected by the App or use of the website unless this Privacy Policy provides different information.

Personal data is information that can be used to identify a person, i.e. information that can be traced back to a person. This typically includes the name, email address or telephone number. In addition, however, purely technical data that can be traced back to a person must also be regarded as personal data.

The following party is responsible for the processing of data collected by this App:

PVRADAR Labs GmbH

Dieding 1, 85560 Ebersberg

The company's data protection officer is: **Kostiantyn Pogorelov**

The company's data protection officer can be contacted at: privacy@pvradar.com

Users' Rights

On request, anyone using the App/Website (hereinafter referred to as '**Users**', which includes Single Users and users of an Organization as defined in the Terms of use) has the **right to obtain free information** on his or her stored personal data. Additionally, Users have the **right to obtain the rectification of inaccurate personal data**, the **right to obtain a restriction of excessively processing of personal data** as well as the **right to obtain the erasure** of unlawful processed personal data or data which is stored too long (as far as there are no legal obligations to store the data). Furthermore, registered Users have the right to receive their personal data in a structured,

commonly used, and machine-readable format and to transmit those data to another controller (**right to data portability**).

Users also have the right to object to the processing of their personal data, which is carried out on the basis of Art. 6 (1) lit. e or f GDPR.

The Operator will then no longer process the personal data relating to Users unless the Operator can demonstrate compelling legitimate reason for the processing which override the Users' interests, rights and freedoms, or the processing serves to assert, exercise or defend legal claims.

In order to exercise their rights, Users can write an email to privacy@pvradar.com.

In addition, Users also have the right **to complain to a data protection supervisory authority.** A list of European data protection authorities and their contact details can be found at the following link: https://edpb.europa.eu/about-edpb/board/members_en.

Data Recipients

Generally, the Operator does not transfer personal data, except when this is mentioned expressively in this Privacy Policy. Nevertheless, the App is hosted by the Operator's service provider Amazon Web Services (“AWS), Oskar-von-Miller-Ring 20, 80333 München. Within this hosting services, AWS automatically processes the abovementioned personal data. This is done exclusively in accordance with instructions and on behalf of the Operator, according to a processing contract, Art. 28 GDPR.

The transfer of personal data to the abovementioned service provider is based on Art. 6 (1) lit. f GDPR. According to Art. 6 (1) lit. f GDPR, the processing of personal data is lawful if the processing is necessary for the purpose of the legitimate interests pursued by the Operator, except where such interests are overridden by Users' interests or fundamental rights and freedoms which require protection of personal data. The Operator's legitimate interest consists in the use of special service providers that realize hosting better than the Operator does. Users can object to this data processing at any time if there are reasons which exist in their particular situation and which speak against the data processing. In order to do so, Users can write an email to the data protection officer.

Information on Cookies

Cookies are small text files which are stored on Users' terminal device by the browser used when using the App. In this way Users can 'recognize' individual services of a website and 'remember'

which settings they have made. This serves on the one hand the user-friendliness of web pages and thus the Users (e.g. storage of login data). On the other hand, cookies are used to collect data on website usage for analysis and remarketing.

Some cookies are automatically deleted from the Users' terminal device as soon as they leave App (so-called session cookie). Other cookies are stored for a certain period of time, which does not exceed two years in each case (persistent cookies). The Operator also uses so-called third-party cookies, which are managed by third parties in order to offer certain services.

You can influence the use of cookies. Most browsers have an option that restricts or completely prevents the storage of cookies. However, it is pointed out that the use and especially the comfort of use are limited without cookies.

Overview about the Processes

Personal data are processed on the App/website in the context of the following processes:

1. Registration (App)
2. Newsletter (App/Website)
3. Contact (App/Website)
4. Server-Logfiles (App/Website)
5. Keycloak (App)
6. Metabase (App)
7. Plausible Analytics (App/Website)
8. Payment using Stripe (Website)

1. Registration

To use the App it is necessary that the User registers himself and provides the following personal data: name and surname, e-mail address, company name.

In case the User is registered on the platform, the User can share data with other users. There are no additional information required when registering on the Platform.

Legal Basis

Account and order details are processed on the basis of Art. 6 (1) lit. b GDPR. According to Art. 6 (1) lit. b GDPR, the processing of personal data is lawful if it is necessary to perform a contract. The provision of Users' personal data is necessary in order to conclude a contract.

Storage Period

The Operator stores the Users' data as long as the contract exists. After receiving the termination notice, the Operator will delete the personal data unless it is obligated to store it according to the applicable law.

2. Email Newsletter

If the User has subscribed to the newsletter, the users email address will be used to send the email newsletter of the Operator. The only personal data that is required to subscribe to the email newsletter is an email address.

Legal Basis

This data processing is based on a consent which Users have given by subscribing to the newsletter. According to Art. 6 (1) lit. a GDPR, the processing of personal data is lawful if the data subject has given consent to the processing of his or her data for one or more specific purposes. Within the frame of subscribing to the newsletter, Users have given the following consent:

"Within the scope of this newsletter, I agree that virtuous-Re regularly provides me with information and news. I can withdraw my consent at any time with effect for the future. In order to do so, I can write an email to privacy@pvradar.com."

Storage Period

Data which is stored within the frame of the newsletter registration will be deleted if Users have successfully unsubscribed from the newsletter.

3. Contact

When Users contact us, for example by email, the provided information will be stored for the purpose of processing the request and in the event that further questions arise.

Legal Basis

The data processing within the frame of contacting is based on Art. 6 (1) lit. f GDPR. According to Art. 6 (1) lit. f GDPR, the processing of personal data is lawful if the processing is necessary for the purpose of the legitimate interests pursued by the Operator, except where such interests are

overridden by Users' interests or fundamental rights and freedoms which require protection of personal data. The Operator's legitimate interest consists in the provision of this App's functions and to provide the fastest solution in case Users have a support request. Users can object to this data processing at any time if there are reasons which exist in their particular situation and which speak against the data processing.

Storage Period

The personal data stored within the scope of establishing contact will be deleted if the request has been completely clarified and it is also not expected that the specific communication will become relevant again in the future.

4. Server Log Files

Each time Users access the App/website, the Operator automatically collects a series of technical data, which is personal data.

These are:

- Users' IP address
- Name of the requested website respectively the data file
- Date and time of the access
- Transferred data volume
- Report of successful retrieval
- User's operating system

This data is not combined with any other personal data. The Operator collects server log files for the purpose of administering the App and to be able to recognize and prevent unauthorized access.

Legal Basis

The data processing within the frame of the log files is based on Art. 6 (1) lit. f GDPR. According to Art. 6 (1) lit. f GDPR, the processing of personal data is lawful if the processing is necessary for the purpose of the legitimate interests pursued by the Operator, except where such interests are overridden by Users' interests or fundamental rights and freedoms which require protection of personal data. The Operator's legitimate interest is in the easier administration and the ability to

detect and track hacking. Users can object to this data processing at any time if there are reasons which exist in their particular situation and which speak against the data processing.

What is an IP address?

The IP address is a worldwide unique sign of numbers which is assigned to each device (e.g. smartphone, tablet, PC) connected to the Internet. Therefore, the IP address depends on which device and which access Users are currently using to be connected to the Internet. This can be the IP address that Users' Internet provider has assigned to them, for example, if they are connected to the Internet via W-LAN at home. It can also be an IP address assigned to Users by their mobile phone provider, or the IP address of a provider of a public or private W-LAN or other Internet access. In its currently most common form (IPv4), the IP address consists of four number blocks. In most cases, as private Users, Users will not use a constant IP address, as this is only temporarily assigned to them by their provider (so-called 'dynamic IP address'). With a permanently assigned IP address (so-called 'static IP address'), a clear assignment of user data is easier in principle. Except for the purpose of tracking unauthorized access to the App, the Operator does not use this data on a personal basis, but only evaluate on an anonymous basis which of the App's pages are favored, how many accesses are made daily and the like.

The App already supports the new IPv6 addresses. If Users already have an IPv6 address, they should also know the following: The IPv6 address consists of eight blocks of four. The first four blocks are, as with the entire IPv4 address, typically assigned dynamically by private Users. However, the last four blocks of an IPv6 address (so-called 'interface identifiers') are determined by the terminal device that Users use. Unless otherwise set in their operating system, the so-called MAC address is used for this. The MAC address is a type of serial number that is assigned uniquely for each IP-capable device worldwide. The Operator does not store the last four blocks of the Users' IPv6 address. The Operator generally recommends that Users activate the so-called 'Privacy Extensions' on their terminal device in order to make the last four blocks of their IPv6 address more anonymous. Most common operating systems have a 'Privacy Extensions' function, which, however, is not present by default in some cases.

Storage Period

The log data is automatically deleted within 14 days. The Operator reserves the right to store log data longer, if there are facts which suggest that an illegal access has taken place (such as the attempt of hacking or a so-called DOS-attack).

5. Keycloak

We are using Keycloak as Identity- and Access management tool for our App. The goal is to verify a single login using the same username and password (single sign-on/SSO). The following data is being processed:

- last name,
- first name,
- Email address,
- the hash value of the user password.

Legal Basis

This data processing is based is based on Art. 6 (1) lit. f GDPR. According to Art. 6 (1) lit. f GDPR, the processing of personal data is lawful if the processing is necessary for the purpose of the legitimate interests pursued by the Operator, except where such interests are overridden by Users' interests or fundamental rights and freedoms which require protection of personal data. The Operator's legitimate interest is to verify that only registered users use the service provided with the App.

Storage duration

The cookie set is deleted after a session.

6. Metabase

We are using the services of Metabase Inc. , 660 4th Street Suite 557, San Francisco, CA 94107, United States as Business Intelligence Tool to in the backend of the App. Metabase is a program to visualize data.

You can find more information under the following link: https://www.metabase.com/privacy

Legal Basis

This data processing is based is based on Art. 6 (1) lit. f GDPR. According to Art. 6 (1) lit. f GDPR, the processing of personal data is lawful if the processing is necessary for the purpose of the legitimate interests pursued by the Operator, except where such interests are overridden by Users' interests or fundamental rights and freedoms which require protection of personal data.

The Operator's legitimate interest is in the easier administration of the App and improvement of the user experience.

Storage duration

We only store anonymized data.

7. Plausible Analytics

In order to understand the use of our website/App and to improve it, we use the web analytics tool Plausible Analytics from the provider Plausible Insights OÜ Västrikutn 2, 50403, Tartu, Estonia, Plausible. In doing so, your browser establishes a connection to the Plausible Analytics servers in the European Union. For technical reasons, your IP address is transmitted to Plausible, where it is processed for one legal second to generate a daily-rotating, anonymous hash that is not stored on your device. A processing of personal data except the IP address does not take place.

Details can be found in the privacy policy of Plausible Analytics: https://plausible.io/data-policy

Legal Basis

This data processing is based on Art. 6 (1) lit. f GDPR. According to Art. 6 (1) lit. f GDPR, the processing of personal data is lawful if the processing is necessary for the purpose of the legitimate interests pursued by the Operator, except where such interests are overridden by Users' interests or fundamental rights and freedoms which require protection of personal data. The Operator's legitimate interest is in the easier administration of the App and improvement of the user experience.

Storage Period

We only store statistical data.

8. Payment using Stripe

We offer payment via the provider Stripe. The provider of this payment service is Stripe Payments Europe, Ltd, The One Building, 1 Grand Canal Street Lower, Dublin 2, Ireland (hereinafter "Stripe"). Stripe collects your contact information as well as payment information such as payment type, credit card number, account numbers and the amounts to be paid. In addition,

Stripe sets cookies to perform the payment process and to ensure the security of the payment process.

We have entered into a data processing agreement with Stripe pursuant to Article 28 GDPR. Due to the fact that Stripe is headquartered in the USA and because payments (depending on the bank or credit institution involved) may be processed outside the European Union. Stripe is registered under the EU US Data Privacy Framework. Any data transfer to the USA is therefore covered by the adequacy decision of the EU commission.

Legal Basis

The transfer of data by us to Stripe is based on Art. 6 (1) lit. f GDPR. According to Art. 6 (1) lit. f GDPR, the processing of personal data is lawful if the processing is necessary for the purpose of the legitimate interests pursued by the Operator, except where such interests are overridden by Users' interests or fundamental rights and freedoms which require protection of personal data. The Operator's legitimate interest is in the easier administration and offering a user-friendly payment method.

Storage Period

We store the data only insofar as this is necessary for invoicing and for compliance with the statutory retention obligations for invoices.