YOUR API KEY

cLIlkTy1kZ4DRqCQlQzoC7FvNj3jh1Ys6UErv6nP

Endpoint: The above API key shall be used only with the endpoints that return more than one model.

Integration: Include the API key in the headers of your server side request, in the **X-API-KEY** field. To keep consumption under the limit, EPREL strongly recommends caching all retrieved data.

For security reasons, EPREL restricts cross-origin HTTP requests, by enabling CORS. Thus, for specific endpoints, calling the EPREL Public API with a frontend client, might result in a null/bad response. For more information, please check the EPREL Public API documentation.

This API key provides access to the **PRODUCTION** environment. If you plan to integrate the EPREL Public API in non-production environment, we recommend mocking the integration, especially in case of load tests.

API Limitations and Inactivation: EPREL sets limits on your use of the APIs, limiting the number of requests that you may make. Your current limit is 5 requests per second. If you want to use the API beyond these limits, please contact EPREL Helpdesk.

EPREL may suspend access to the API without notice, if we reasonably believe that you are in violation of the Terms and Conditions.

Communication: EPREL may send communications in connection with your use of the APIs. For such communication, the email address indicated in the request form will be used.

Monitoring: The API is designed to help you enhance your websites and applications. EPREL team will monitor the use of the API to ensure quality of service. This monitoring may include EPREL accessing and using your API Client, for example to identify or troubleshoot security or integration issues.

API Security and Prohibitions: When integrating and using the API, you should not:

- Disclose the API key to a third party. EPREL strongly recommends that you restrict your API key by limiting the usage to those needed for your application.
- Interfere with or disrupt the API or the servers or networks providing the API.
- Reverse engineer or attempt to extract the source code from the API or any related software.
- API key and credentials are intended to be used by you and identify your API Client. You will keep your credentials confidential and make reasonable efforts to prevent and discourage other API Clients from using your credentials.