Axopar

PRIVACY NOTICE

Employees

1. General information

The purpose of this Privacy Notice is to inform the employees of Axopar Boats Oy (later "Employer" or "we") how we process your personal data; what personal data we collect, how the data is used and to whom the data is disclosed. In addition, this Privacy Notice informs you how you can control the processing of your personal data.

We are dedicated to protect the privacy of our employees and commit to adhere to the provisions of the European Union's General Data Protection Regulation (later "GDPR") (2016/679) and applicable national laws concerning the processing of the personal data of the employees.

This Privacy Notice applies to persons employed by Axopar and, where applicable, to former employees, to the Chief Executive Officer who has entered into a director agreement with the Axopar and other persons in similar positions with a director agreement (later "Employees", "data subjects" or "you").

Personal data refers to information, which allows a person to be directly or indirectly identified as an individual person. Examples of Personal data: name, email address, date of birth and Internet Protocol (IP) address of a personal computer (PC).

1.1. Controller

Company: Axopar Boats Oy
Business ID: 2611096-1
Address: Itämerentori 2, 00180 Helsinki

Email: privacy@axopar.fi

1.2. Point of contact

Data privacy (and HR) responsible: Anne Hakala
Phone: +358 40 560 7901

2. Purpose and legal basis of the processing of personal data

The purpose of processing of the personal data of the Employee is to exercise the Employee's and Employer's rights and obligations related to the employment and to perform the duties of the Employer.

The data can be used for the following purposes:

- Manage the rights and obligations of the Employer and the Employees (such as management of the payments, vacations and other absences, insurances, health care and benefits)
- Monitor the performance of the duties of the employment relationship and ensure compliance with applicable employment laws and other legal obligations
- Fulfil legal obligations including fraud prevention
- Ensure the security and safety of the premises, data and property
- IT environment and access management, information security
- Managing performance appraisals and other evaluations
- Development of the Employee career paths (such as training)

- Benefit and event management
- Internal planning and development

The legal bases of the processing of the Employee's personal data are the contract of employment between the Employee and the Employer and managing the legal obligations related to the rights and obligations of the parties, as well as ensuring the security and safety.

The Employer also processes personal data for exercising the legitimate interests of the Employee and the Employer to support the Employees career development, manage benefits and events, plan and develop the work and work environments, and to protect data and property.

When the Employee submits personal data that is not mandatory but voluntary information, the legal basis is consent. The Employee can withdraw his/her consent at any time (see later, Rights of the data subjects (Employees)).

3. Processing of personal data and legal basis

The Employer collects and processes only personal data which is necessary for the performance of the employment and to manage related rights and obligations of both parties, as well as the benefits offered to the Employees. This concerns the information the Employees give to the Employer as well as information gathered from other possible sources.

The Personal Data we collect/receive are retained for the period necessary to fulfil the purposes outlined in this Privacy Notice unless a longer retention period is required by law (e.g. specific legislation, accounting or reporting requirements or obligations). We may retain the data longer if necessary to resolve possible disputes. The retention periods depend on the purpose of the processing and type of the information.

When the personal data is no longer needed for the purposes described in this Privacy Notice the data will be deleted within a reasonable timeframe.

Personal data processed and the retention periods:

Categories of personal data	**Example of data**	**Retention period or criteria used to determine the period**
Contact and identity information	Name, date of birth and contact details, personal identification code or other corresponding national id and date of birth, employment contract data	11 years after the termination of the employment
Salary, benefits and expenses related data	Payment and documentation related to the calculation of salaries, deductions, benefits and travel expenses, tax card or similar document based on national tax law	11 years after the end of the fiscal year
Vacation and absence data	Information of vacations and other possible absences	7 years
Working hour data	Information on working hours	7 years
Performance appraisal and performance evaluation data	Information related to performance appraisals, skills surveys and courses	7 years

Sensitive personal data: • Sick leave data and ability to work • Trade union data (voluntarily collected data)	medical certificates, evaluation of the ability to work trade union membership can be submitted for direct payments to the trade union (applies only to the employees working in Finland)	Sick leave data and ability to work: 7 years as a maximum Trade union payments related data: 11 years after the end of the fiscal year Trade union membership data: removed upon employee request
Travelling data	Work related travelling information, bookings and other arrangements, passport number	As long as the booking is valid, the related payments have been processed and the expenses have been entered to the accounting system
IT management and security related data	IP address, access credentials and logs	Retention times are determined in the relevant IT management and security policies/procedures/guidelines
Background screening data (participation requires consent)	Security screening or credit check results	Security screening: 6 months as a maximum Credit check: 6 months as a maximum
Education data (voluntary)	Exams, diplomas, certificates, previous work history, courses and training, and information on the CV and job application	Until the termination of the employment
Additional voluntary data	Wishes and preferences related to work and company benefits and events	The Employer will remove the data when the employment is terminated, upon employee request, or if the data is no longer needed for the purposes it was collected

The personal collected are mainly mandatory due to the legal obligations of the Employer and obligations related to the employment. Failure to give requested mandatory personal data may restrict the performance of the employment contract such as the processing of the salaries and benefits, and granting promotions.

Requests for security screening and credit check are based on the employee consent. However, if the employee refuses to participate in those background checks, this may affect the employees contract of employment.

Sources of personal data:

The primary source of personal data is the relevant Employee. The Employer does not collect any personal data from third parties without a consent of the Employee or without a legal basis.

4. Recipients of personal data

The Employer transfers personal data to payroll and related services and for fulfilling the legal obligations of the Employer such as insurance and company health care.

Personal data is disclosed to the following recipients:

- Statutory recipients such as tax authorities

- Insurance companies: LähiTapiola Keskinäinen Vakuutusyhtiö
- Pension insurance: Keskinäinen Työeläkevakuutusyhtiö Elo
- Insurance broker: Oy Risk Consult AB
- Health care: Terveystalo Oy
- Mobile phones and internet: Telia Finland Oyj
- Company credit cards: Nordea Business MasterCard
- Travel agency: Dream time holidays Oy
- CFO services: Greenstep Oy
- Company benefits partners: Secto Automotive Oy (car leasing), Edenred Finland Oy (lunch vouchers)
- IT systems/service providers: Visma Solution Oy (Netvisor), Dropbox International Unlimite (Dropbox), Office IT services including equipment (R.O Data Service), Microsoft (Microsoft 365, email and other office services)
- Other services: Kiinteistö Oy Itämerentori (physical access management service provider for the premises)

Other transfers

In a case of emergency or other surprising occasions, the Employer may need to disclose the personal data to protect lives and health, and rights and property. The Employer may also disclose the personal data to exercise legal claims.

The Employer can be obliged to transfer personal data to the third parties involved in any merger, sale of our assets, or other similar arrangements. The Employer will continue to ensure the confidentiality of the personal data of the Employees and give appropriate notice to the Employees.

The Employer does not disclose the personal data of the Employees to third parties for direct marketing, market research or polls without a consent of the Employee.

Transfer outside EU/EEA

The Employer does not transfer personal data of the Employees to countries outside the European Union (EU) or the European Economic Area (EEA). However, the recipients may have operations outside EU/EEA. If personal data are transferred outside EU/EEA, the transfer is secured by legal measures, appropriate safeguards.

5. Protection of Personal Data

We commit to follow to the security provisions of applicable data protection regulations, as well as to process Personal data in compliance with good processing practices.

Personal data are protected with appropriate technical and organizational measures. We store the information in secured IT-environments that are protected with adequate security technics. Our personnel and processors that process personal data are obliged to keep the personal data strictly confidential. Access to personal data is only granted to those employees that need the information to perform their work tasks. Employees and processors have personal IDs and passwords.

We inform the authorities and users of data breaches according to applicable information security and data protection regulation(s).

6. Rights of the data subjects (Employees)

You have the rights set out in the applicable data protection legislation.

- You have the right to have confirmed if we process your personal data.

- You have the right to verify and access your personal data and to request us to provide you the data in writing or electronically
- You have the right to have corrected any incorrect or incomplete personal data. You have also the right to request us to remove data
- You have the right to transmit to another controller the personal data you have provided (based on your consent or contract relationship)
- You have the right to request us to restrict processing of your personal data in accordance with the conditions set out in the data protection legislation
- You have the right to object to processing of your personal data for certain purposes e.g. you have the right to deny any processing or transferring of data for direct marketing
- If the processing of your personal data is based on consent, you have the right to withdraw consent at any time (the withdrawal does not affect the lawfulness of processing based on consent before its withdrawal)

You can use your rights by submitting a request to the contact information in the beginning of this Privacy Notice. After receiving all the required information of your request (incl. confirmation of identity), we will start the processing of your request. We will do our best effort to process your request within a period of one month.

We may reject requests that are unreasonably repetitive, excessive or clearly abusive (manifestly unfounded).

Right to lodge a complaint to the supervisory authority

In case you consider our processing activities of your Personal data to be inconsistent with the data protection legislation, you have the right to lodge a complaint to the competent (data protection) supervisory authority.

7. Changes to this Privacy Notice

We may have to change or update this Privacy Notice from time to time, whenever necessary. The need for a change may arise from changes in the legislation. We recommend you to read this Privacy Notice regularly. All changes hereto will be made available on our internal communication channels. In addition, we will also inform you by email of any significant changes affecting your rights.

This Privacy Notice has been published on May 31th, v1.0

Change history

Version number	Change description	Date