

# DATA PROTECTION POLICY for Employees

(last updated: **04/2025**)

**Dear Employee,**

With this data protection policy, we aim to inform you about the type, scope, and purpose of the personal data we process and to clarify the rights you are entitled to in this context.

This data protection policy applies exclusively to data processing by the data controllers, not to the data processing by third parties, which do not fall under the controllers mentioned below.

The data controller for the data processing listed below is **Porsche Holding GmbH** for employees who are in direct employment with Porsche Holding GmbH. For employees who are directly employed by other group companies, Porsche Holding GmbH carries out the data processing on behalf of the individual data controllers listed in point 3.2.14 (as a data processor for the individual data controllers listed).

These group companies are themselves independent data controllers (hereinafter referred to as "**data controllers**") and do not act as joint data controllers. The individual data controllers can be found listed at the end of this data protection policy.

## 1. Data Security

The data controllers have taken appropriate technical and organisational measures to protect your data from loss, manipulation, or unauthorised access. These measures are regularly reviewed and continuously adapted to the state of the art. If there is a breach of the protection of your personal data that is likely to result in a high risk to your rights and freedoms, we will notify you immediately and, if possible, within 72 hours.

## 2. Data Transfer

### 2.1. Partners

The data controllers do not carry out some data processing themselves but receive support from professional partners who act on behalf of the data controllers. The partners ensure that the processing of your personal data complies with data protection regulations and guarantees your rights. The partners are not permitted to use the provided personal data for their own or advertising purposes or to pass it on to third parties. Furthermore, the data controller does not pass on data to third parties, such as address publishers and direct mail companies.

### 2.2. Recipients

#### 2.2.1. Transfer of data to external recipients

Transfer of relevant data, as required by law or contractual agreement, to:

- Krankenversicherungsträger (ÖGK)
- Allgemeine Unfallversicherungsanstalt (AUVA)
- Finanzamt (FA)
- Generali Versicherung AG

- FAO Group GmbH
- Externe Trainer
- Wirtschaftskammer Österreich (WKO)
- Österreichische Gewerkschaftskammer (ÖGK)
- Uniqa Österreich Versicherung AG
- VBV-Pensionskasse AG
- Betriebsärzte
- Raiffeisen Bank International AG
- Pensionsversicherungsanstalt PVA
- IT

#### **2.2.2. Transfer of data to internal recipients:**

- VW AG
- Works Council
- Management
- Associated group companies

### **3. Data Processing in the context of Employment**

#### **3.1. Personnel Administration & Employment Relationship**

##### **3.1.1. Recruitment & Selection Processes**

**Description:** Processing of applicant data for job advertisements, selection processes, interviews, feedback, and apprentice knowledge tests. The application documents are shared with the HR department and management to select suitable candidates.

**Data categories:** Private contact and identification data, professional contact and organizational data, IT usage data, sensitive personal data (Art. 9 GDPR, e.g., health data, union membership), salary and time management data, special category: employee photo (for internal applications)

**Purpose:** Recruitment/training of employees

**Legal basis:** Art. 6 (1) a) consent, Art. 6 (1) b) fulfilment of a contract, Art. 6 (1) f) legitimate interest. The legitimate interest lies in the internal administrative purposes of the group.

**Storage duration:**

- Rejected applicants: 7 months (6 months according to the Equal Treatment Act (GIBG), § 15 Para. 1 GIBG + 1 month).
- Employed applicants: Transfer to the personnel file, deletion of the data at the end of the employment relationship according to the statutory retention period.

##### **3.1.2. Management/administration of employment relationships**

**Description:** Electronic storage of application documents, creation of an employment contract using text block software, creation and maintenance of an employee account, entry in the employee entry database, printing of the employee card, change of master data (address, bank details, marital status), change of employment relationship (parental leave, maternity leave, parental leave, etc.), salary change (collective agreement, individual changes, reclassifications), resignation of employees, removal of the employee profile/account in SAP HR, entry in the employee exit database.

**Data categories:** Private contact and identification data, data on personal/professional relationships & characteristics, special category: employee photo, sensitive personal data (Art. 9 GDPR) or data on criminal convictions, salary and time management data.

**Purpose:** Management of the employment relationship

**Legal basis:** Art. 6 (1) b) fulfilment of a contract, Art. 6 (1) c) fulfilment of a legal obligation, Art. 6 (1) f) legitimate interest. The processing to fulfil a legal obligation is based on tax, social security, and labour law regulations (§ 26 ArbVG, § 7i ASVG, etc.). The legitimate interest lies in the internal administrative purposes of the group.

**Storage duration:**

- 7 years from the end of the calendar year (§ 132 BAO) for books and records and the documents belonging to the books and records (e.g., payment proof for payroll payments)
- 30 years from the end of the employment relationship (§ 39 AngG in conjunction with § 1479 ABGB) for the data required for issuing a service certificate (e.g., name, type and duration of employment, evaluation).
- Periods according to the IT security concept for log data.

### 3.1.3. Time recording

**Description:** Time recording, control of approval authorisations for time corrections, leave applications, and sickness notifications.

**Data categories:** Private contact and identification data, data on personal/professional relationships & characteristics, sensitive personal data (Art. 9 GDPR) or data on criminal convictions, salary and time management data.

**Purpose:** Management of the employment relationship

**Legal basis:** Art. 6 (1) b) fulfilment of a contract, Art. 6 (1) c) fulfilment of a legal obligation. The processing to fulfil a legal obligation is based on labour law regulations (§ 26 Para. 1 Z 3 ArbVG, § 16 Para. 2 AZG, etc.).

**Storage duration:** 7 years from the end of the calendar year (§ 132 BAO) for books and records and the documents belonging to the books and records (e.g., payment proof for payroll payments).

### 3.1.4. Payroll

**Description:** Payroll accounting, ongoing and variable bonuses and deductions (overtime, meal deductions, parking deck, etc.), sending the payroll statement, transfers, error checking, including backup & archiving. Salaries are paid monthly by Raiffeisen Bank International AG, Vienna.

**Data categories:** Salary and time management data, data on personal/professional relationships & characteristics, IT usage data, sensitive personal data (Art. 9 GDPR), credit and bank data.

**Purpose:** Payroll

**Legal basis:** Art. 6 (1) b) fulfilment of a contract, Art. 6 (1) c) fulfilment of a legal obligation. The processing to fulfil a legal obligation is based on tax, social security, and labour law regulations (§ 132 BAO, § 41 EStG, § 4 Para. 1 ASVG, § 2 Z 4b AVRAG, etc.).

**Storage duration:** 7 years from the end of the calendar year (§ 132 BAO) for books and records and the documents belonging to the books and records (e.g., payment proof for payroll payments).

### 3.1.5. Travel expense accounting

**Description:** Accounting of travel expenses and control of approval authorisations for travel expense accounting.

**Data categories:** Credit and bank data, salary and time management data.

**Purpose:** Management of the employment relationship.

**Legal basis:** Art. 6 (1) c) fulfilment of a legal obligation, Art. 6 (1) b) fulfilment of a contract. The processing to fulfil a legal obligation is based on tax regulations (§ 132 BAO, § 1 Para. 1 Z 1 EstG, etc.).

**Storage duration:** 7 years from the end of the calendar year (§ 132 BAO) for books and records and the documents belonging to the books and records (e.g., payment proof for payroll payments).

### **3.1.6. Issuance of a service certificate**

**Description:** Every employee is entitled to a service certificate. The service certificate (final certificate, interim certificate) can be requested and created in the intranet via the Haufe Certificate Manager by the employee or their supervisor. The request is first processed by the HR department (recruiting), and then the supervisor is asked by email to further process the certificate (especially the evaluation of the employee). The employee can also process the certificate themselves. After that, the certificate is finalised by the HR department and Haufe and given for signing (signature by personnel support and AL/HAL). PIA companies are excluded from this process. The managers of the PIA fill out an evaluation form (pdf or Word) and send it to the responsible personnel officer. They then manually write the service certificate and send it to the employee.

**Data categories:** Data on personal/professional relationships & characteristics, professional contact and organisational data.

**Purpose:** Employee performance evaluation, management of the employment relationship.

**Legal basis:** Art. 6 (1) c) fulfilment of a legal obligation. The processing to fulfil a legal obligation is based on § 39 AngG & § 146 ABGB.

**Storage duration:** 30 years after the employee's departure. The service certificates created in the certificate manager are stored in the digital personnel file after completion.

### **3.1.7. Transmission of employee data to internal systems**

**Description:** Transmission of employee data to internal systems (e.g., Partner.Net, Lotus Notes databases, Synertrade, Kira) for the identification of employees and the assignment of access and usage rights.

**Data categories:** Professional contact and organisational data, data on personal/professional relationships & characteristics.

**Purpose:** Management of the employment relationship, identity and access management.

**Legal basis:** Art. 6 (1) b) fulfilment of a contract, Art. 6 (1) f) legitimate interest. The legitimate interest lies in the internal administrative purposes of the group.

**Storage duration:** Until the end of the employment relationship.

### **3.1.8. Employee ID card**

**Description:** In the context of creating and issuing employee ID cards, personal data is processed on the card. These cards contain the employee's name, an employee ID, and a photo on the front. No personal

data is stored on the chip of the card. The card is used for access to company premises and systems and for identification within the company.

**Data categories:** Professional contact and organisational data, special category: employee photo.

**Purpose:** Management of the employment relationship.

**Legal basis:** Art. 6 (1) b) fulfilment of a contract.

**Storage duration:** 2 weeks after the employee leaves the company.

### **3.1.9. Access to employee data on a case-by-case basis**

**Description:** In certain cases, it may be necessary to access employee email accounts or view certain emails. Access is always carried out jointly by the data protection department and the works council. Information to the affected employees is given on a case-by-case basis and as quickly as possible after the actual access.

Application cases for access to employee email accounts may include:

- Requests for information from data subjects (legal obligation)
- Unplanned absences/unplanned departure of employees according to the works agreement (legitimate interest)
- Other security-relevant incidents, e.g., hacker attacks (legitimate interest)

Depending on the application case, the email search is carried out by POI.

**Data categories:** Professional contact and organisational data.

**Purpose:** Compliance.

**Legal basis:** Art. 6 (1) c) fulfilment of a legal obligation, Art. 6 (1) f) legitimate interest. The processing to fulfil a legal obligation is based on Art. 15 GDPR.

**Storage duration:**

- For requests for information: 3 years; storage together with the documentation of the data subject's request.
- For other access: generally, no storage, or it may vary depending on the necessary documentation (e.g., data breach documentation).

### **3.1.10. Processing of voluntary information**

**Description:** In the context of the employment relationship, union membership or emergency contact details may be processed. These data are provided voluntarily. Union membership is processed for the purpose of transferring the union contribution through the employer. Emergency contacts are processed to contact a relative in emergency situations.

**Data categories:** Private contact and identification data, data on personal/professional relationships & characteristics, sensitive personal data (Art. 9 GDPR).

**Purpose:** Management of the employment relationship.

**Legal basis:** Art. 6 (1) c) fulfilment of a legal obligation; Art. 6 (1) f) legitimate interest. The legitimate interest lies in protecting the health and safety of employees. The processing to fulfil a legal obligation is based on § 62 EstG.

**Storage duration:** Until the end of the employment relationship.

## **3.2. Social & Insurance matters**

### **3.2.1. Notification to the tax office**

**Description:** Notification to the tax office upon termination of employment, calculation of tax.

**Data categories:** Private contact and identification data, salary and time management data.

**Purpose:** Management of the employment relationship.

**Legal basis:** Art. 6 (1) c) fulfilment of a legal obligation. The processing to fulfil a legal obligation is based on tax regulations (§ 41 EStG, § 82 EStG, etc.).

**Storage duration:** 7 years from the end of the calendar year (§ 132 BAO) for books and records and the documents belonging to the books and records (e.g., payment proof for payroll payments).

### **3.2.2. Insurance notification**

**Description:** Notification upon start of employment, notification upon termination of employment, contribution declaration monthly, contribution fund accounting annually.

**Data categories:** Private contact and identification data, data on personal/professional relationships & characteristics, salary and time management data, data on personal/professional relationships & characteristics.

**Purpose:** Insurance processing.

**Legal basis:** Art. 6 (1) c) fulfilment of a legal obligation. The processing to fulfil a legal obligation is based on social security regulations (§ 33 ASVG, § 34 ASVG, etc.).

**Storage duration:** 7 years from the end of the calendar year (§ 132 BAO) for books and records and the documents belonging to the books and records (e.g., payment proof for payroll payments).

### **3.2.3. Notification to the Chamber of Commerce (WKO)**

**Description:** Notification to the Chambers of Commerce (apprentices) at the start of the employment relationship, notification to the Chambers of Commerce (apprentices) at the end of the employment relationship.

**Data categories:** Data from apprentices: Private contact and identification data, data on personal/professional relationships & characteristics, salary and time management data.

**Purpose:** Management of the employment relationship.

**Legal basis:** Art. 6 (1) c) fulfilment of a legal obligation. The processing to fulfil a legal obligation is based on § 19 BAG & § 13 BAG.

**Storage duration:** 7 years from the end of the calendar year (§ 132 BAO) for books and records and the documents belonging to the books and records (e.g., payment proof for payroll payments).

### **3.2.4. Accident notification via Quentic**

**Description:** Accident notifications are created and transmitted to the AUVA. The required personal data is transferred via an SAP interface and entered into the accident notification form.

**Data categories:** Sensitive personal data (Art. 9 GDPR), private contact and identification data.

**Purpose:** Insurance processing.

**Legal basis:** Art. 6 (1) c) fulfilment of a legal obligation. The processing to fulfil a legal obligation is based on social security regulations (§ 363 ASVG, etc.).

**Storage duration:** 5 years.

### **3.2.5. Pension insurance (PVA)**

**Description:** As part of the statutory obligations for social security and pension provision, the company regularly transmits personal data of its employees to the Pension Insurance Institution (PVA). These data are collected by the payroll department and forwarded to the PVA to correctly record contribution periods and contribution-related information. Data processing is carried out exclusively for the purpose of fulfilling legal obligations, especially in connection with social and pension insurance. This is a routine, legally required transmission.

**Data categories:** Data on personal/professional relationships & characteristics, salary and time management data.

**Purpose:** Insurance processing.

**Legal basis:** Art. 6 (1) c) fulfilment of a legal obligation. The processing to fulfil a legal obligation is based on social security regulations (§ 33 ASVG, § 36 ASVG, § 223 ASVG, etc.).

**Storage duration:**

- 7 years for ongoing payroll data.
- 100 years for documents related to pension commitments.
- 30 years for paper files of employees who left before 2018, as a service certificate can be requested up to 30 years after the end of the service relationship.

### **3.2.6. Company pension scheme**

**Description:** Due to a contractual obligation (pension fund contract / pension commitment), personal data is processed for the purpose of managing and paying company pensions for entitled persons (AWB) and beneficiaries (LB). In the event of the death of an AWB/LB, the survivor is reinvested in the system. Annual contributions for the beneficiaries and the creation of annual information are automatically calculated. Pension payments are made through the payroll department.

**Data categories:** Private contact and identification data, data on personal/professional relationships & characteristics, salary and time management data, credit and bank data.

**Purpose:** Management and determination of entitlements and benefits.

**Legal basis:** Art. 6 (1) b) fulfilment of a contract.

**Storage duration:** 30 years from the last payment to the last beneficiary for data that can be assigned to the pension fund contract.

### **3.2.7. Data transfer to private insurance companies**

**Description:** Each month, the contact and identification data of employees are transferred in the form of an SAP-HR extract as a .csv file to the Generali Versicherung AG to manage insurance contracts. This is done centrally by the holding company on behalf of the group companies.

**Data categories:** Private contact and identification data.

**Purpose:** Management of the insurance contract.

**Legal basis:** Art. 6 (1) b) fulfilment of a contract.

**Storage duration:** Until the end of the insurance period.

### **3.2.8. Data transfer to external providers for health offers registration**

**Description:** By registering for a health offer, personal data is transferred to external providers (company doctor, trainer, etc.) (registration for health offers, details of agreed or available appointments, cancellation and rescheduling of appointments, and general information about health offers).

**Data categories:** Professional contact and organisational data, sensitive personal data (Art. 9 GDPR).

**Purpose:** Registration for health offers.

**Legal basis:** Art. 6 (1) b) fulfilment of a contract.

**Storage duration:** 7 years from the end of the calendar year (§ 132 BAO) for books and records and the documents belonging to the books and records (e.g., payment proof for payroll payments).

### **3.2.9. Internal provision of employee information for organization & communication**

**Description:** In order to contact colleagues, the contact details are internally published in the ORG portal and the telephone directory.

**Data categories:** Professional contact and (work) organisational data, data on personal/professional circumstances & characteristics, special category: employee photo.

**Purpose:** Communication (internal).

**Legal basis:** Art. 6 (1) f) Legitimate interest. The legitimate interest lies in efficient internal communication.

**Storage duration:** Until the end of the employment.

### **3.2.10. Creation and Publication of Employee Magazines**

**Description:** Quarterly mapping of personal data (employee photos and names) into various employee information magazines (PMI) for internal informational purposes. The data is sourced from SAP-HR via Excel file export. The PMI is available in both printed and electronic forms (stored on the PHS file server).

**Data categories:** Private contact and identification data, data on personal/professional circumstances & characteristics.

**Purpose:** Information for employees.

**Legal basis:** Art. 6 (1) f) Legitimate interest. The legitimate interest lies in the data exchange within the corporate group for internal administrative purposes.



**Storage duration:** The data is retained for historical documentation purposes and only stored as long as it is required for this purpose. This may mean long-term storage, as long as the historical value of the data is given. The publication of this personal data constitutes press products according to the Media Act, which comply with the legal requirements of press law (media privilege).

**Data categories:** Professional contact and (work) organisational data, data on personal/professional circumstances & characteristics, special category: employee photo.

**Purpose:** Communication (internal).

**Legal basis:** Art. 6 (1) f) Legitimate interest. The legitimate interest lies in efficient internal communication.

Storage duration: Until the end of the employment.

### 3.2.11. Archiving and Usage of Employee Photos on Company Platforms

**Description:** Archive photos are processed for reporting on anniversaries, events, and other occasions and are published exclusively on internal company platforms.

**Data categories:** Special category: employee photo.

**Purpose:** Communication (internal).

**Legal basis:** Art. 6 (1) f) Legitimate interest. The legitimate interest lies in internal communication within the group.

**Storage duration:** The data is retained for historical documentation and stored for as long as it is required for this purpose. This may mean long-term storage, as long as the historical value of the data is given.

### 3.2.12. Press Releases and Information

**Description:** Processing includes the creation and publication of press releases and related information. In particular, for the entry and departure of executives, the press releases may contain personal data.

**Data categories:** Data on personal/professional circumstances & characteristics, professional contact and (work) organisational data.

**Purpose:** Communication (internal/external).

**Legal basis:** Art. 6 (1) f) Legitimate interest. The legitimate interest lies in transparent communication about company developments.

**Storage duration:** The data is retained for historical documentation and stored for as long as it is required for this purpose. This may mean long-term storage, as long as the historical value of the data is given. The publication of this personal data constitutes press products according to the Media Act, which comply with the legal requirements of press law (media privilege).

### 3.2.13. Internal Reporting and Business Analysis

**Description:** Business-relevant data is collected, processed, and visualised in reporting tools for internal reporting and business analysis. This serves to analyse company metrics, support decision-making, and optimise internal processes. The data is loaded from various sources (ERP, CRM, or dealer management systems) into a data warehouse via ETL processes and then made available in reporting and analysis platforms like Power BI or similar systems.

**Data categories:** Professional contact and (work) organisational data.

**Purpose:** Reporting.

**Legal basis:** Art. 6 (1) f) Legitimate interest. The legitimate interest lies in data exchange within the corporate group to optimise business processes.

**Storage duration:** The data is stored according to the deletion concepts of the respective source systems and deleted after its purpose is achieved, generally after 7 years.

**Legal basis:** Art. 6 (1) f) Legitimate interest. The legitimate interest lies in data exchange within the corporate group for internal administrative purposes.

**Storage duration:** 3 years for information requests.

Otherwise, no storage occurs or varies depending on necessary documentation (e.g., data breach documentation).

#### **3.2.14. Data Transfer to the Works Council**

**Description:** Upon an employee's entry or exit from the company, the employee data sheet is transferred to the works council. The works council checks whether an employee is assigned to the correct employment group according to the collective bargaining agreement and qualifications.

**Data categories:** Contact and identification data, data on personal/professional circumstances & characteristics, remuneration and time management data.

**Purpose:** Employment processing.

**Legal basis:** Art. 6 (1) c) Fulfilment of a legal obligation. The processing for fulfilment of a legal obligation arises from § 78 ArbVG.

**Storage duration:** 3 years.

### **3.3. Compliance & Security**

#### **3.3.1. Recording and Investigation of Whistleblower Reports**

**Description:** The controller processes personal data to investigate and clarify internal irregularities within the company. Whistleblower reports are directly reported to the VW Investigations Office. Depending on the category of the reports, specific instructions are forwarded by the VW Investigations Office to the relevant department in PHS (Compliance Department) for processing and documentation.

**Data categories:** Private contact and identification data, data on personal/professional circumstances & characteristics, credit and bank data, private contact and identification data, IT usage data, sensitive personal data (Art. 9 GDPR) or data on criminal convictions.

**Purpose:** Compliance.

**Legal basis:** Art. 6 (1) c) Fulfilment of a legal obligation, Art. 6 (1) f) Legitimate interest. The processing for fulfilment of a legal obligation arises from the Whistleblower Protection Act. The legitimate interest lies in data exchange within the corporate group for internal administrative purposes.

**Storage duration:** 5 years according to § 8 Abs. 11 HSchG. Additionally, as long as necessary for administrative or civil proceedings or to protect the whistleblower, the person affected by the whistleblowing, or others involved in or affected by subsequent measures. Log data: 3 years.

### 3.3.2. Incentives

**Description:** Due to legal regulations against corruption and internal compliance guidelines, donations (invitations, gifts, etc.) are documented in the Incentive App, and an approval process is carried out. All donations to and from third parties with business relevance are transparently documented.

**Data categories:** Professional contact and (work) organisational data, IT usage data.

**Purpose:** Release and documentation of donations to internal and external receivers.

**Legal basis:** Art. 6 (1) f) Legitimate interest. The legitimate interest lies in data exchange within the corporate group for internal administrative purposes and fraud prevention.

**Storage duration:** 7 years.

### 3.3.3. Background and Sanctions List Check

**Description:** During the application process and the filling of positions, applicants and employees undergo a background check. This includes internal background checks (for internal positions), comprehensive background checks with external service providers (for executives), and comparison with current sanctions lists (EU, UN, OFAC lists) to ensure no connection to listed persons or organisations.

**Data categories:** Contract data, data on personal/professional circumstances & characteristics, professional contact and (work) organisational data, sensitive personal data (Art. 9 GDPR) or data on criminal convictions.

**Purpose:** Compliance, fraud prevention.

**Legal basis:** Art. 6 (1) f) Legitimate interest. The legitimate interest lies in fraud prevention and security checks.

**Storage duration:**

- Data of applicants: 6 months after completion of the application process.
- Data of employed executives: No later than 3 years after the end of employment.
- Data from the sanctions list check: 1 year after the employee's exit date.

### 3.3.4. Protocol of Committee Meetings

**Description:** Creation, management, and archiving of protocols for meetings and resolutions of various committees (e.g., supervisory board, management board, works council, specialised committees).

**Purpose:** Compliance.

**Data categories:** Professional contact and (work) organisational data, data on personal/professional circumstances & characteristics.

**Legal basis:** Art. 6 (1) c) Fulfilment of a legal obligation. The processing for fulfilment of a legal obligation arises from commercial and corporate law provisions (§ 212 UGB, § 132 BAO, etc.).

**Storage duration:** 7 years (§ 212 UGB, § 132 BAO).

### 3.3.5. Management and Updating of Corporate Data

**Description:** Processing of data for the establishment, management, and modification of companies and to ensure the up-to-date status of corporate data. This includes:

- Creation, management, and archiving of relevant corporate documents (e.g., company formations and contracts, resolutions, capital measures, company register entries).
- Publication and archiving of annual financial statements.
- Management of essential contracts (e.g., importer contracts).
- Conducting change-of-control queries.
- Documentation and updating of corporate master data and shareholder and director information in internal systems.

**Data categories:** Contract data, professional contact and (work) organisational data, data on personal/professional circumstances & characteristics.

**Purpose:** Processing of contract data, compliance.

**Legal basis:** Art. 6 (1) c) Fulfilment of a legal obligation, Art. 6 (1) f) Legitimate interest. The processing for fulfilment of a legal obligation arises from commercial and corporate law provisions (§ 189 UGB, § 10 FBG, § 9 GmbHG, etc.). The legitimate interest lies in the proper management and organisation of the company.

**Storage duration:**

- Corporate documents and contracts: Duration of the company, but at least 7 years according to § 212 UGB (Commercial Code) and tax retention periods.
- Resolutions and annual financial statements: 10 years according to tax and commercial law requirements.
- Data on corporate functions: 3 years after the end of the function, unless longer legal retention periods apply.

### 3.3.6. Declaration and Disclosure Obligations

**Description:** In certain cases, relevant data is requested by authorities or contractual partners to fulfil legal or contractual declaration and/or disclosure obligations (e.g., data of directors of affected companies).

**Data categories:** Professional contact and (work) organisational data, data on personal/professional circumstances & characteristics, contract data, credit and bank data.

**Purpose:** Compliance.

**Legal basis:** Art. 6 (1) b) Fulfilment of a contract, Art. 6 (1) c) Fulfilment of a legal obligation. The processing for fulfilment of a legal obligation arises from commercial and corporate law provisions (§ 189 UGB, § 10 FBG, § 9 GmbHG, etc.).

**Storage duration:** For books and records and accompanying documents (e.g., payment evidence for accounting payments): 7 years from the end of the calendar year (§ 132 BAO).

### 3.3.7. Video Surveillance System Porschehof & TVZ

**Description:** Operation of video surveillance systems at Porschehof and TVZ Wals.

**Data categories:** Image and sound recordings (e.g., video surveillance, event photography, etc.).

**Purpose:** Video surveillance.

**Legal basis:** Art. 6 (1) f) Legitimate interest. The legitimate interest lies in ensuring the safety of people and property.

**Storage duration:** 5 days.

### **3.4. Training & Development**

#### **3.4.1. Potential Analysis (Captain Aptitude Test)**

**Description:** Collection of contact data and self-reports and their processing as part of an online potential analysis, specifically through conducting an aptitude test for defined groups (e.g., aspiring executives, Basic Lead); including backup and archiving.

**Data categories:** Professional contact and (work) organisational data.

**Purpose:** Employee training.

**Legal basis:** Art. 6 (1) f) Legitimate interest. The legitimate interest lies in identifying potential executives.

**Storage duration:** Until the end of the employment.

#### **3.4.2. Creation of a Short Biography**

**Description:** Creation of an internal short biography for defined groups.

**Data categories:** Data on personal/professional circumstances & characteristics, private contact and identification data, special category: employee photo.

**Purpose:** Employee training.

**Legal basis:** Art. 6 (1) f) Legitimate interest. The legitimate interest lies in data exchange within the corporate group for internal administrative purposes.

**Storage duration:** Until the end of the employment.

#### **3.4.3. Mood Barometer (Stibam)**

**Description:** Conducting the annual employee satisfaction survey and follow-up processes to measure employee sentiment as a basis for organisational development processes. The department (Personnel Development) receives an extract from SAP-HR with data including first and last name, personnel number, and data on the employee's organisational assignment. This extract is uploaded to the Volkswagen STIBA system for comparison with the available data in the Volkswagen VCD system. After reconciliation, a user ID and password are generated for each employee in the system and sent electronically by the department (Personnel Development) via email and - if no company email exists - in writing to all employees. Includes backup and archiving.

**Data categories:** IT usage data, professional contact and (work) organisational data.

**Purpose:** Assessment of job satisfaction.

**Legal basis:** Art. 6 (1) f) Legitimate interest. The legitimate interest lies in data exchange within the corporate group for internal administrative purposes.

**Storage duration:**

- The attendance list is stored as long as the reports are released.
- Knowledge of the processing notice for extended purpose binding and administrative data (e.g., log files for Stiba coordinators) is stored for one year.
- The pinboard entries and the permission/structure list are stored for 2 years.
- Measures for sustainable implementation and representative roles are stored for 7 years after creation.

#### **3.4.4. Employee Development Programmes**

**Description:** Conducting development programmes for high potentials within the company. These are accompanied by external trainers and personnel development. To better get to know the participants, there are interviews with participants at the beginning and during the programme. After completing the development programme, a written report is created for each participant by the external trainers, which includes the first and last name and current position in the company. Additionally, explanations of their skills and a potential assessment are formulated. The report is received by the participant, personnel development, and management. Examples of employee development programmes: Trainee Development International, Basic Lead Development, Highline Development.

**Data categories:** Professional contact and (work) organisational data.

**Purpose:** Employee training.

**Legal basis:** Art. 6 (1) f) Legitimate interest. The legitimate interest lies in data exchange within the corporate group for internal administrative purposes.

**Storage duration:** Until the end of the employment.

#### **3.4.5. Employee Training**

**Description:** Employees and executives participate in training measures that include both face-to-face training with external trainers and digital eLearning programmes.

For face-to-face training, trainers receive a participant list including name and company. Examples include competency training, Management Compact, and the Finance Academy.

Employees also complete mandatory eLearning programmes in the Compliance Lotus Notes database (e.g., antitrust and competition law, data protection) with a final knowledge test. The departments evaluate the name and completion time of the participants.

**Data categories:** Professional contact and (work) organisational data.

**Purpose:** Employee training.

**Legal basis:** Art. 6 (1) f) Legitimate interest. The legitimate interest lies in data exchange within the corporate group for internal administrative purposes.

**Storage duration:** Until the end of the employment.

#### **3.4.6. Digital Employee Interviews (DigiMAG)**

**Description:** The digital employee interview (DigiMAG) is an annual process for the structured recording and assessment of employees' performance, development potential, and career goals. The interview results are documented and processed. This information is transmitted to personnel development to enable comprehensive analysis.

**Data categories:** Data on personal/professional circumstances & characteristics, professional contact and (work) organisational data.

**Purpose:** Employment processing.

**Legal basis:** Art. 6 (1) f) Legitimate interest. The legitimate interest lies in personnel development and performance assessment.

**Storage duration:** 3 years.

#### **3.4.7. Registration and Licence Management for Speexx**

**Description:** During the use of the language learning app Speexx, registration and licence management data are collected and processed. The registration is carried out via a forms survey in which name, personnel number, company, country, billing address or cost centre, and the approver are requested. These data are used exclusively for internal administration, particularly for registration overview and billing control, and are not passed on to Speexx. After approval, the access to the platform is automatically provided. Authentication is carried out via single sign-on with the company email address. For licence management, the duration of use and the status of the licences are recorded to ensure efficient administration and control.

**Data categories:** Professional contact and (work) organisational data.

**Purpose:** Employee training.

**Legal basis:** Art. 6 (1) f) Legitimate interest. The legitimate interest lies in the administration and control of licence usage.

**Storage duration:** 3 years.

#### **3.4.8. Management by Expertise Programme**

**Description:** Participants in the Management by Expertise (MBE) programme receive a forms survey for self-assessment before their module, which is sent by Porsche Holding GmbH personnel development. The completed surveys are forwarded to the trainers of ComTeam Organisationsentwicklung GmbH, who evaluate the results. The individual evaluation is made available to the participants on the first day of the module.

**Data categories:** Professional contact and (work) organisational data.

**Purpose:** Employee training.

**Legal basis:** Art. 6 (1) f) Legitimate interest. The legitimate interest lies in data exchange within the corporate group for internal administrative purposes.

**Storage duration:** The personal data are processed until the transmission of the evaluation to the participants on the first day of the module. Afterwards, the data are completely deleted.

### **3.5. Childcare & Social Services**

#### **3.5.1. Company Kindergarten & Kids Club**

**Description:** The company kindergarten offers year-round childcare for employees' children. Additionally, the Kids Club takes place during the holiday periods, a multi-week care programme with special leisure activities. For the registration and organisation of care, personal data of the children, such as name, date of birth, and insurance number, are collected. To ensure safe and appropriate care, sensitive data like allergies, intolerances, immunisation status, or special care needs may also be processed. During care, photos of participating children may be taken for souvenir purposes or internal documentation. The exact programme varies depending on the number of participants, individual needs, and organisational conditions.

**Data categories:** Private contact and identification data, data on personal/professional circumstances & characteristics, sensitive personal data (Art. 9 GDPR) or data on criminal convictions.

**Purpose:** Childcare.

**Legal basis:** Art. 6 (1) a) Consent.

**Storage duration:** Registration forms with immunisation data, intolerances etc. are only needed until the end of the event, additional personal data like name, personnel number, email, etc. are needed for billing up to 6 months after the end of the event. Invoices have a statutory retention period of 7 years but contain no sensitive data.

### **3.6. Marketing & Employer Branding**

#### **3.6.1. Employer Branding**

**Description:** All activities to position PHS as an attractive employer on the market (using TikTok, YouTube, Instagram, Facebook, LinkedIn...). Includes employee photos.

**Data categories:** Private contact and identification data.

**Purpose:** Marketing.

**Legal basis:** Art. 6 (1) a) Consent, Art. 6 (1) f) Legitimate interest. The legitimate interest lies in direct marketing.

**Storage duration:** Until the end of the employment.

### **3.7. Finance & Property Management**

#### **3.7.1. Financial Accounting**

**Description:** Recording all payment transactions and valuations in a company.

**Data categories:** Private contact and identification data, accounting data according to the law, remuneration and time management data.

**Purpose:** Accounting and settlement.

**Legal basis:** Art. 6 (1) b) Fulfilment of a contract, Art. 6 (1) c) Fulfilment of a legal obligation. The processing for fulfilment of a legal obligation arises from tax and corporate law provisions (§ 124 BAO, § 189 UGB, § 4 Abs. 3 and 4 EStG, etc.).

**Storage duration:** 7 years from the end of the calendar year (§ 132 BAO) for books and records and accompanying documents (e.g., payment evidence for accounting payments).

#### **3.7.2. Real Estate Management**

**Description:** The processing activity includes the management of real estate and the settlement of rents for land and buildings using the Easy program from Andromeda. Master data is maintained here, including contracts (e.g. building rights contracts, rental contracts, also from third parties), property and unit value notices, building permits, and other agreements.

**Data categories:** Contract data

**Purpose:** Processing of contract data

**Legal basis:** Art. 6 (1) b) Fulfillment of a contract



**Storage period:** 22 years

## **4. Your Rights**

You are entitled to the following rights:

### **4.1. General Rights**

**Right to information:** You can request confirmation as to whether and to what extent your data is being processed.

**Right to correction:** If we process incomplete or incorrect data about you, you can request its correction or completion at any time.

**Right to deletion:** You can request the deletion of your data if the purpose for which it was collected no longer exists, if the processing is unlawful, if the processing unjustifiably interferes with your legitimate protection interests, or if the data processing is based on your consent and you have withdrawn it. Note that there may be other reasons that prevent the immediate deletion of your data, such as legally regulated retention obligations, ongoing proceedings, assertion, exercise, or defense of legal claims, etc.

**Right to restriction of processing:** You have the right to request the restriction of the processing of your data if you dispute the accuracy of your data, for a period that allows us to verify the accuracy of the data, if the processing of your data is unlawful, but you refuse deletion and instead request the restriction of data use, if we no longer need the data for the intended purpose, but you still need this data to assert, exercise, or defend legal claims, or if you have objected to the processing of the data as long as it is not yet clear whether our legitimate reasons outweigh yours.

**Right to data portability:** You can request that we provide you with the data you have provided to us in a structured, commonly used, and machine-readable format, or that we transmit this data to another controller without hindrance from us, provided we process the data based on your given consent or to fulfill a contract between us and the processing is carried out using automated procedures.

**Right to objection:** If we process your data to perform tasks that are in the public interest, to exercise official authority, or if we rely on the necessity to protect our legitimate interest, you can object to this data processing provided there is an overriding protection interest in your data.

To exercise these rights, please contact the contact details provided in point 7.

### **4.2. Rights within the framework of consent**

You can withdraw consent declarations given to us at any time without giving reasons, with each individual consent declaration being revocable independently of other consent declarations given to us.

We explicitly point out that a withdrawal has no immediate or indirect negative consequences for your employment with us. A withdrawal only means that we can no longer process your data for the purposes mentioned in the respective consent declaration from that point on, and that any rights and/or benefits associated with the processing of the specific data (if any) can no longer be claimed.

For a withdrawal, please contact the contact details provided in point 7.

### **4.3. Right to complain**

If you believe that the processing of your data violates data protection law or that your data protection rights have otherwise been violated in any way, please feel free to contact us (contact details see point 7).

Of course, you can also file a complaint with the Austrian Data Protection Authority (for more information: [www.dsb.gv.at](http://www.dsb.gv.at)).

## **5. Subsidiaries of Porsche Holding GmbH**

- **Porsche Holding GmbH** (Louise-Piëch-Straße 2, 5020 Salzburg)  
**Porsche Immobilien GmbH** (Louise-Piëch-Straße 2, 5020 Salzburg)  
**Porsche Air Service GmbH** (Louise-Piëch-Straße 2, 5020 Salzburg)  
**PoHo Clearing GmbH** mit Sitz in 83395 Freilassing  
**Porsche Corporate Finance GmbH** (Louise-Piëch-Straße 2, 5020 Salzburg)
- **Porsche Austria GmbH & Co OG** (Louise-Piëch-Straße 2, 5020 Salzburg)  
**Porsche Konstruktionen GmbH & Co KG** (Louise-Piëch-Straße 2, 5020 Salzburg)  
**Allmobil GmbH** (Louise-Piëch-Straße 2, 5020 Salzburg)  
**Porsche Media & Creative GmbH** (Louise-Piëch-Straße 2, 5020 Salzburg)  
**Moon Power GmbH** (Louise-Piëch-Straße 2, 5020 Salzburg)
- **Porsche Versicherungs AG (Vogelweiderstraße 75, 5020 Salzburg)**  
**Porsche Mobility GmbH (Trattnerhof 1, 1010 Wien)**  
  
**ARAC GmbH** (Louise-Piëch-Straße 2, 5020 Salzburg)
- **Volkswagen-Versicherungsdienst GmbH (Trattnerhof 1, 1010 Wien)**
- **Porsche Inter Auto GmbH & Co KG** (Louise-Piëch-Straße 2, 5020 Salzburg)  
**Exclusive Cars Vertriebs GmbH (Ketzergasse 120, 1230 Wien)**  
**Bikes Vertriebs GmbH (Ketzergasse 120, 1230 Wien)**
- **Porsche Informatik GmbH** (Louise-Piëch-Straße 2, 5020 Salzburg)  
**DigiLab Porsche Informatik GmbH (Rothschildplatz 3, 1020 Wien)**

## **6. Contact Information**

All rights can be directly exercised at Porsche Holding GmbH by sending a notification to the email address [Datenschutz-Personal@porsche.co.at](mailto:Datenschutz-Personal@porsche.co.at).