

department / area	Title of the process	Status of document
YACHT-POOL	Concept for data processing	<i>Final</i>



This document is a translation. In case of doubt, the German original version applies.

Concerned persons	
	Name
responsible:	Dr. Friedrich Schöchl
author:	Andreas Lang
further contributors:	Daniel Prusinski
quality controlled by:	Dr. Holger Mühlbauer

Table of Content

1. LEGAL BASE
2. AIM OF THIS YACHT-POOL-DS-CONCEPT
3. PREAMBLE
4. DATA PROCESSING POLICY AND RESPONSIBILITIES WITHIN THE COMPANY
5. LEGAL FRAMEWORK IN THE COMPANY
6. DATA PROCESSING - IMPACT ASSESSMENT AND DOCUMENTATION
7. EXISTING TECHNICAL AND ORGANISATIONAL PROCEDURES (TOM)

department / area	Title of the process	Status of document
YACHT-POOL	Concept for data processing	<i>Final</i>



1 LEGAL BASE

<https://www.activemind.de/datenschutz/dokumente/datenschutzkonzept/>

Who needs a concept for data protection?

DSGVO states in Art. 5 (2) the principle of **accountability**. According to this, every responsible department has to proof, that an **overall concept to comply with data protection** is present. The responsible department has to check on that regularly and develop and modify it, if necessary.

Art. 32 states the requirements regarding **security of data processing**.

In other words: Companies that process personal data, **must install a procedure to check on** the effectiveness of the data protection and data security measures **regularly, as well as assess and evaluate** this procedure. Therefore, a data protection concept is a perfect starting position.

What is the content of a data protection concept?

A data protection concept should:

- have a good **structure**, because it has to be understood by internal and external stakeholders.
- It also has to reflect the **individual conditions** of a company. Therefore, templates or patterns must always be adapted to the individual case. However, the following content should be found in a data protection concept:
 - **data protection policy and responsibilities** within the company
 - **legal framework** in the company
 - **documentation**
 - existing **technical and organisational actions**
 - IT-authorisation concept, IT-usage guidelines
 - **organisational minimum rules**

2 AIM OF THIS YACHT-POOL-DS-CONCEPT

The purpose of the data protection concept is to present the data protection aspects in a comprehensive documentation. It serves as a basis for data protection checks and can be used for example by the customer in the context of order processing. The YACHT-POOL-DS concept not only ensures compliance with the European General Data Protection Regulation (DSGVO), but also provides proof of compliance. The purpose of the data protection measures taken by YACHT-POOL is to ensure the availability of data, integrity, confidentiality, non-interchangeability through purpose, transparency through auditability and intervability through anchor points.

3 PREAMBLE

YACHT POOL was founded in 1976 by Dr. Friedrich Schöch, who still heads the company as managing director.

YACHT-POOL is the inventor of skipper liability insurance and all charter insurances, and has introduced the "all-risks coverage" in private hull comprehensive insurance.

YACHT-POOL understands its founding philosophy as the "pool of customers" that has been a strong counterweight to the asymmetric relationship between customers and the big, powerful insurance companies for over 40 years. YACHT-POOL has always learned from its customers and has developed into a recognized innovator and expert. The direct communication between the YACHT-POOL crew with skippers and yacht owners results in inspiration, mutual benefit and high customer loyalty and satisfaction.

YACHT-POOL uses this unique know-how in the insurance industry in cooperation with all players of the charter and yacht industry.

This resulted in a unique, international network and acceptance as a cross-company, cross-border solution specialist and expert in the industry. As a result, YACHT-POOL has the position in many areas much like a consumer protection organization in the charter industry.

department / area	Title of the process	Status of document
YACHT-POOL	Concept for data processing	<i>Final</i>



Due to this self-conception, respectability and thus the protection of the personal data of all customers and business partners, has an outstanding value for the reputation of YACHT-POOL.

4 DATA PROCESSING POLICY AND RESPONSIBILITIES WITHIN THE COMPANY

The Federal Data Protection Act (BDSG) and the General Data Protection Regulation (DSGVO) serve YACHT-POOL as the legal basis for data processing operations in which the consent of the persons concerned for a specific processing purpose is necessary and available. For the use of the services, e.g. the conclusion and fulfillment of an insurance contract, the processing of personal data by YACHT-POOL and affiliated companies (insurers and banks) is necessary.

Personal data processed and necessary data used by YACHT-POOL are:

- salutation (hence gender)
- surname, name
- year of birth
- address
- if applicable further contact details (E-Mail / Fax)
- bank details/credit card details
- registration number of the vessel („license number“)
- driver's license numbers
- insurance numbers

The provision of this data is contractually required and mandatory for conclusion of contract and contract execution.

YACHT-POOL is committed to the principle of data economy. This means that we only ask for the data of customers that are absolutely necessary for the respective processing purpose. To generate statistics (for example, to develop new tariffs) or to comply with regulatory or contractual obligations, we anonymise personal information as early and as far as possible.

The protection of customer and business partner data has always been a top priority for YACHT-POOL. YACHT-POOL is aware of the trust of its customers and business partners and regards this as a high good.

Every employee of YACHT-POOL is obliged to privacy and has made corresponding contractual statements. Overall responsibility for all DS matters is the managing director. He determines the operationally responsible persons in the individual case.

Through internal efforts and external consultants and professionals, YACHT-POOL is working to continuously improve the privacy management system.

This also means that all employees are trained in regular training and discussions and are sensitized for the DS problem.

Data protection officer

Currently no data protection officer for one or all companies of the "YACHT-POOL Group" is necessary. This decision was made after examination of the requirements according to Art. 37 DSGVO and the requirements according to § 4f BDSG-old as well as § 38 BDSG-new.

Concrete justification:

YACHT-POOL is not an authority or a public body, YACHT-POOL does not carry out any core activity with extensive or systematic monitoring of persons or with extensive processing of particularly sensitive data (Articles 9, 10 DS-GVO). Furthermore, in a YACHT-POOL company, fewer than ten people are generally involved in the automated processing of personal data and no processing is carried out that is subject to a data protection impact assessment according to Art. 35 DS-GVO. YACHT-POOL does not process personal data for business purposes for the purpose of transmission, anonymized transmission or for market or opinion research purposes.

5 LEGAL FRAMEWORK IN THE COMPANY

The legal framework of YACHT-POOL's activities and thus the handling of personal data is governed by numerous laws and regulations.

department / area	Title of the process	Status of document
YACHT-POOL	Concept for data processing	<i>Final</i>



These include in non-exhaustive list the BGB, VVG, IDD, UWG, the mediator's guideline and last but not least BDSG (new) and the DSGVO.

Further requirements exist through contracts with external parties, e.g. insurers who are all within the scope of the GDPR and apply the same strict standards for the protection of personal data as YACHT-POOL.

Within the companies of the "YACHT-POOL-Group" there are traditionally organizational and personal requirements for regular order data processing. The joint management of all companies of the "YACHT-POOL Group" and the corresponding order DP contracts ensure the high standards of data protection throughout the country.

6 DATA PROCESSING - IMPACT ASSESSMENT AND DOCUMENTATION

YACHT-POOL has assessed the risks to the rights and freedoms of individuals from possible misuse of data, as well as the likelihood of their occurrence. It follows that a DS Impact Assessment according to Art. 35 is not necessary. Since the necessary personal data are very limited and to a large extent publicly accessible (→ 4) a correct, wrong or abusive processing can not result in

- physical or psychological damage
- material or immaterial harm and if so, only in a very limited way
- discrimination, significant economic or social disadvantages, the loss of rights and freedoms are unimaginable.
- Inadvertent or unlawful destruction, loss, alteration or unauthorized disclosure of personal data can not result in physical, psychological or material or immaterial damage.

Therefore, there is a normal requirement for the protection requirement and the documentation. YACHT-POOL considers bank details / credit card details as the most sensitive data.

Internal reviews are normally carried out every 3 months, external reviews are not planned at this time.

7 EXISTING TECHNICAL AND ORGANISATORICAL ACTIONS (TOM)

Measures of pseudonymisation and encryption of personal data are carried out, which ensure a current level of protection. Likewise, our measures for data security have the goal of a permanent, high resilience of our systems and services with regard to the associated data processing. We ensure the ability to rapidly restore the availability of and access to personal information in the event of a physical or technical incident.

We also use a process to periodically review, evaluate and evaluate the effectiveness of the technical and organizational measures to ensure the safety of the data processing. In addition, the controller and the processor take steps to ensure that individuals under their responsibility who have access to personal data are only processing them at the direction of the controller, unless they are obliged to process them under the law of the Union or the Member States.

The business processes of YACHT-POOL are based on the specifications of Art. 32 of the General Data Protection Regulation (DSGVO). The measures taken in the company ensure that unauthorized persons can not influence such data processing systems on which personal data are processed or stored.

Access control: No unauthorized access to data processing systems

YACHT-POOL denies unauthorized persons access to and access to data processing equipment used to process or secure personal data by:

- Documented key assignment, definition of authorized persons
- Access to the office space only by or in the company of authorized persons
- Central access control for office space (key concept)
- Fire alarm system (in planning)
- Monitoring equipment / alarm system (in planning)
- Store confidential documents only in lockable cabinets.

department / area	Title of the process	Status of document
YACHT-POOL	Concept for data processing	<i>Final</i>



Access Control: No unauthorized system usage

YACHT-POOL prevents unauthorized persons from using the data processing systems through the following measures:

- Setting up an account per user
- Password protection:
Passwords with min. 8 characters incl. Two special characters. Passwords are changed every 90 days.
- IP limited access to server
- Securing the IT systems and networks against external access (for example through firewalls)
- Regular check of the validity of the access authorizations
- Logging of accesses (for example through event logs)
- Securing the workstations in the absence
- Encryption of mobile data carriers (including backup systems)

Access and Delivery Control: No unauthorized reading, copying, modification or removal

The confidentiality and integrity measures taken in the company ensure that those entitled to use a data processing system only have access to the data subject to their access authorization. In addition, it ensures that personal data can not be read, copied, altered or removed without authorization during processing, use and after storage.

- differentiated and task-related authorizations (for example, profiles, roles, transactions, separation of user and admin accounts)
- defining the access rights (for example, reading, changing, deleting, evaluating, administrating)
- regularly check the validity of the assigned permissions
- definition of personnel responsibilities

The measures taken in the company ensure sufficient follow-up control. Personal data this way is not possibly illegally read, copied, altered or removed during the electronic transmission or during its transport or storage on data carriers without it being checked, determined and prevented.

YACHT-POOL hereby assures that no data will be passed on to third parties beyond the statutory exceptions. The measures taken to achieve this objective are listed below:

- pass-through Control: No unauthorized reading, copying, modification or removal during electronic transmission or transport
- encryption
- determining the transmission paths and data recipients
- electronic signature
- transport security (for example, sealed shipping, password protection for file transfer)
- Virtual Private Network (VPN), tunnel connection
- Commitment of all employees to privacy secrecy and telecommunications secrecy.
- there are regulations for data destruction and deletion (deletion concept)

Pseudonymisation

For the purpose of the analysis of personal data (statistics, billing, forwarding to insurers), the data will be exported to e.g. Excel lists and anonymized as far as possible.

Integrity

The data integrity measures taken within the company ensure sufficient input control. It can be retrospectively reviewed in YACHT-POOL's business processes to determine if and by whom personal data has been entered, altered or removed from the data processing systems.

This is done by the following measures:

- warranty by logging and logging system
- definition of responsibilities for input

department / area	Title of the process	Status of document
YACHT-POOL	Concept for data processing	<i>Final</i>



The measures taken within the company also ensure a high level of protection in the area of contract control. The personal data processed in the order will only be processed in accordance with the instructions of the client.

This is supported by the following measures:

- written contract for order processing acc. Art. 28 DSGVO with regulations on the rights and obligations of the contractor and client
- formalized order placement

The company's separation control measures also ensure that personal data collected for a variety of purposes can also be processed separately.

Availability and resilience

The availability control measures taken in the company ensure that personal data is protected against accidental destruction or loss, or that rapid recoverability is ensured.

- 2x backup procedure daily
- antivirus / firewall
- emergency plan
- regular software updates
- separate storage of the backup copies
- conduct a vulnerability analysis on hardware and software regularly

Procedures for periodic review, assessment and evaluation

- privacy management
- privacy-friendly presets
- definition of criteria for selecting contractors
- incident response management
- clear contract design
- regular monitoring of contract execution by contractors

We carry out regular reviews of the risk analysis and the technical and organizational measures and adapt them to the state of the art.

valid from	valid until	description of type of modification	distributed to personnel on / by
25.5.2018	unlimited	new release	