Personal Data Protection Statement

1. INTRODUCTION

We, HENNLICH s.r.o., with its registered office at Českolipská 9, 412 01 Litoměřice, ID: 14869446, tax ID: CZ14869446, recorded in the Commercial Register held by County Court in Ústí nad Labem, file no. C 274, have prepared this Personal Data Protection Statement to inform you how we collect, process, use and protect your personal data and consequently help protect your privacy.

We handle all your personal data in line with the applicable legislation, primarily Regulation (EU) 2016/679 of the European Parliament and of the Council, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – "**GDPR**"), Act No. 127/2005 Coll., on Electronic Communications, as amended, and Act No. 480/2004 Coll., on Certain Information Society Services, as amended.

Concurrently, we would like to use this Personal Data Protection Statement to clarify the most important terms and processes that we use for the protection of your personal data and answer the questions that you may have in connection with the collection, processing and storing of your personal data.

2. SUPERVISION

We make every effort to adhere to all stipulated and binding rules and safety measures when handling your personal data; for this reason, we believe that no situations will occur that could possibly make you unhappy about our behaviour towards you.

If you do not agree with the manner used by us to process your personal data, you can contact:

Office for Personal Data Protection
Pplk. Sochora 27
170 00 Prague 7
Czech Republic
+420 234 665 111
www.uoou.cz

3. OUR APPROACH

We see personal data protection as essential and we pay considerable attention to it.

You can thus be assured that we handle your personal data with due care and in line with applicable legal regulations and we protect your personal data in the maximum possible scope corresponding to the state-of-the-art technical level.

Personal Data Protection Statement

To fully understand how we protect your personal data, we recommend that you carefully read this **Personal Data Protection Statement**.

In processing your personal data, we adhere to the following principles:

- **Principle of lawfulness** which requires us to process your personal data always in line with legal regulations and pursuant to no fewer than one legal basis.
- **Principle of fairness and transparency** that requires us to process your personal data in an open and transparent manner and provide you with information on the manner of their processing and information to whom your personal data will be disclosed (for example if your personal data are stored on data storage sites – clouds – outside of the European Union and the European Economic Area). This additionally involves our obligation to inform you of cases of serious security breaches or personal data leaks.
- **Principle of purpose limitation** which allows us to collect your personal data only with a clearly defined purpose.
- **Principle of data minimisation** which requires us to process only personal data that are necessary, relevant and adequate in relation to the purpose of their use.
- **Principle of accuracy** which requires us to adopt all reasonable measures allowing us to regularly update or rectify your personal data.
- **Principle of storage limitation** which requires us to store your personal data only for the period that is necessary for the specific purpose for which they are processed (for example over the period for which a marketing consent was granted, if it was not withdrawn before the expiration of this period). As soon as the period for processing expires or the purpose of processing ceases to exist, we erase your personal data or anonymise them, i.e. modify them so that they are not connectable to you.
- **Principle of integrity and confidentiality, incontestability and availability** which requires us to secure your personal data and protect them against unauthorised or illegal processing, loss or destruction. For these reasons, we adopt numerous technical and organisational measures for the protection of your personal data. Concurrently, we ensure that access to your personal data is granted only to selected employees.
- **Principle of responsibility (accountability)** which requires us to be able to document compliance with all the conditions referred to above.

4. CONTACT FOR YOUR QUESTIONS OR CONCERNS

Should there be any vagueness in any part of this Statement or should you have any questions or comments regarding the protection of your personal data, do not hesitate to contact our Personal Data Department:

HENNLICH s.r.o.
Personal Data Department
Českolipská 9
412 01 Litoměřice
Czech Republic
mailto:gdpr@hennlich.cz

5. WHAT ARE PERSONAL DATA, THEIR CATEGORISATION

Personal data are the information that allows us to identify you. Therefore, it includes information that is specifically attributable to you.
Personal data do not include anonymous or aggregated data, i.e. data that cannot be clearly attributed to you.
Personal data are classified into:

- **Basic data** which include, for example, your name, surname, date of birth, number of identity card (another identity document).
- **Special category** of personal data that includes sensitive data which are data of a highly personal nature including, for example, information on your health.

Basic data are further divided into individual categories, the list of which is available in chapter "**15. Categories of personal data**".

6. LEGAL BASIS FOR PROCESSING YOUR PERSONAL DATA

We obtain your personal data from you and further handle them only in the necessary scope and to achieve a certain purpose. The transfer of your personal data is voluntary for you and when their transfer is based on a consent, erasure of processed personal data may be requested when certain conditions are met (for details refer to chapter "**10. Your Rights**").

Personal Data Protection Statement

In certain cases, such as conclusion of a purchase contract for the acquisition of our goods or service, we need to obtain the necessary scope of personal data from you already with your binding order of these goods or service. Without these data, we are unable to meet your requirements and conclude the above contract with you, primarily in terms of compliance with our legislative obligations, and in respect of the protection of our legitimate interests.

Below, we list the lawful bases stipulated by the legislation based on which we are authorised to process your personal data. The principal bases for the processing of your personal data include the following:

- **Consent** – you give us consent for one or several specific purposes (for example for sending commercial messages).
  To obtain the consent with the processing of your personal data, we adhere to the following rules: i) we always collect consents with processing your personal data from you individually, giving the consent thus will not be part of the text of a contract or another arrangement, ii) the text of the consent will always be comprehensible, iii) consent will always be given as a result of your active behaviour, it means no boxes will be pre-filled for you, iv) for each processing purpose you will give your consent individually.

- **Performance of the contract** – we need your personal data for the conclusion of the contract and subsequent performance of the contract, or before the conclusion of the contract (e.g. order preceding the conclusion of a purchase contract).

- **Compliance with the legal obligation** – we need your personal data for their processing to comply with our legislative obligation as a controller.

- **Legitimate interest** – processing your personal data would be necessary for the purposes of our legitimate interests, however, except for cases when your interests or your fundamental rights and freedoms prevail over these interests.

Rather marginally, the following basis will be used for processing your personal data:

- **Protection of interests of data subjects** – processing your personal data would be necessary for the protection of your vital interests or vital interests of another person.

- **Public interest** – we are obliged to process your personal data to accomplish our task performed in the public interest or exercise of public authority for which we will be authorised as the controller.

7. METHODS OF PERSONAL DATA PROCESSING

For details on the methods that we use to process your personal data, please visit our website.

8. REASONS FOR PERSONAL DATA PROCESSING

As we discussed in chapter "**6. Legal basis for processing your personal data**", it is necessary that we have legal basis for each processing of your personal data.

Below you will find examples of situations in which we will most frequently require your personal data and the legal basis for our requirement:

- **Ordering and purchase of a goods** – the legal basis shall be represented by the conclusion and performance of the contract, or performance before the conclusion of the purchase contract.
- **Maintenance services** – the legal basis shall be represented by the conclusion and performance of the contract, or performance before the conclusion of the maintenance contract and provision of the service.
- **Marketing purposes** – the legal basis shall be represented by giving consent to new customers or legitimate interest in the existing ones for the purpose of sending commercial announcement
- **Storage of cookies necessary for the operations of websites** – the legal basis shall be represented by our legitimate interest as the storage of cookies is necessary for the due operation of websites.

9. PERSONAL DATA PROTECTION

We give due care to your personal data protection; for this reason, we adhere to the below listed technical and organisational measures ensuring the security of your personal data. These measures include:

- **Physical access control** – we store all data in a manner to protect access to them, it means that places where data are stored are secured by technical means such as smart cards, keys, electronically lockable door etc.

- **Controlled access** – access to personal data storing systems is not granted to anyone without the relevant password or two-factor verification, data are thus accessible only to authorised persons.

- **Access control** – we have adopted measures that prevent unauthorised reading, copying, modification, removal from the system or other dealing with them.

- **Creation of pseudonyms** – we process personal data by modifying them into a form in which they are not attributable to a specific person (they are pseudonymised).

- **Control of the transfer** – all dealing with personal data in their electronic transfer is protected to prevent unauthorised reading, copying, modification or erasure.

10. YOUR RIGHTS

No personal data protection would be complete if you did not have rights to data protection. Please find below the list of your rights relating to personal data protection along with the practical explanation of their use:

- **Right for the provision of information on personal data processing**
  Entitles you to obtain information relating to our full identification as the controller of your personal data, together with contact data to our personal data officer. Concurrently, you are entitled to know the legal basis for processing (e.g. performance of the contract), purpose (e.g. contracts for the purchase of our goods) or information on the period of personal data storage. We will always inform you on the legal basis and purpose of the personal data processing before we start to process them.

- **Right to access personal data**
  Entitles you to obtain the information whether we process your personal data and if we do so, in what scope. Concurrently, you have the right to request a copy of the processed personal data. Upon your request, we are also obliged to inform you on the purpose of data processing, recipient of processed personal data, or other related information.

- **Right to rectification**
  Will allow you, for example, to ask us to change any of your personal data that we process if it has changed (e.g. change in the surname, change in the address, etc.).

  We, as the personal data controller, are not obliged to actively ascertain whether the personal

data that we collect are up to date, incorrect or inaccurate, however when you notify us about such fact, it is our obligation to deal with your comment or request for rectification. Under similar terms, you have the right to ask us to amend your personal data.

- **Right to erasure**
  Also called the “right to be forgotten” requires us, as the personal data controller, to liquidate your personal data, in the following cases:

1. The purpose of processing no longer exists (e.g. termination of the contract);
2. You withdraw your consent with personal data processing and there is no other reason for processing your personal data (e.g. withdrawal of the marketing consent provided that you have not concluded, for example, a contract with us);
3. You object to personal data processing (provided it is allowable and there are no legal grounds for processing your personal data); and
4. In accordance with the applicable legislation, we are required to erase your data (e.g. obligation to shred).

- **Right to object**
  Is analogous to the right for withdrawal of the consent and will apply when personal data are processed pursuant to a legitimate interest (e.g. for the purpose of protecting your property). You may also object when your personal data are processed for the purpose of direct marketing. In justified cases, your personal data will be erased when the objection is acknowledged and we will no longer process them.

- **Right for data portability**
  If you ask us to transfer your personal data to another controller, we are obliged to do so and transfer them in a structured, commonly used and machine-readable format. You may exercise this right only when the processing is based on the consent or contract and concurrently it is automated, i.e. processing solely made using technical means based on a pre-determined algorithm and without any human intervention.

11. WHO IS THE CONTROLLER AND THE PROCESSOR AND WHAT THEY DO

In cases when you provide us with your personal data, for example in the purchase of our goods or services, when you communicate with us in our marketing campaigns or ask us questions, or you make a complaint regarding the goods or services, we deal with you from the position of your personal data controller.

As the personal data controller, we determine the purpose and means of your personal data processing.

Processing involves any operation with your personal data, for example their collection, processing, organisation, structuring, etc.

As the controller of your personal data, we are concurrently responsible for compliance with all obligations and principles relating to personal data protection, primarily their sufficient protection. If the security of your personal data is breached, which we naturally seek to prevent, we are obliged to communicate this fact to the Office for the Protection of Personal Data within 72 hours.

If the breach of your personal data security involves a significant risk, we are also obliged to communicate this fact to you provided we have your up-to-date contact information available.

The processor is an entity to which we, as the controller, transfer your personal data and which further handles them in line with instructions provided by us. These, for example, include our business partners, typically external marketing agencies that send you commercial and marketing messages on our behalf.

To ensure that your personal data are handled in line with the applicable legislation and are sufficiently secured, we concluded a written contract for personal data processing with the processor.

12. RULES FOR SHARING YOUR PERSONAL DATA WITH THIRD PARTIES

The rules used for sharing your personal data with their processors are divided into two basic categories.

The first category includes sharing personal data in the European Union and European Economic Area, the second category includes sharing with third countries outside the territory of the European Union and European Economic Area and sharing with international organisations.

To be able to share your personal data with the processor in the European Union and European Economic Area, we take care to ensure that this involves:

- Sharing personal data for a specific purpose (e.g. preparation of a marketing campaign);
- Transfer of only a clearly defined and necessary scope of personal data;
- Transfer based on a duly concluded contract for personal data processing; and
- Sharing made in a secured manner (encrypting, pseudonymisation, etc.).

When your personal data are shared with third countries outside the European Union and European Economic Area and international organisations, they are shared solely based on standard contractual clauses, i.e. template contract issued by the European Commission and these will exclusively include entities based in countries that ensure adequate personal data protection according to the resolution of the European Commission. Third countries with which your personal data may be shared will most frequently include the People's Republic of China, India and the Russian Federation.

13. WHEN YOU ARE A DATA SUBJECT

You are a data subject solely as the natural person; legal regulation regarding personal data protection does not apply to legal persons, cooperatives, associations, etc.

Pursuant to these legal basis, we may include you in two basic groups. We see the first group as our customers. You become our customer when your personal data are processed for the conclusion and performance of contracts for the purchase and use of our goods and services.

The second group of personal data subjects we process is the group of third parties. You will be a third party for example when you give us marketing consent or use our website without wanting to be our customer. If you want to know when and under what conditions you may know the scope of your personal data we process, please read chapter "**10. Your Rights**", in which individual procedures and their conditions are explained.

14. GLOSSARY OF TERMS

Sensitive data
Data of a special nature, such as the information on your health or biometrical data allowing the identification of a person (currently called by the legislation "special categories of personal data").

Cookies
Short text file that a visited website sends to the browser. It allows the web to record information on your visit, for example the preferred language and other settings. The next visit of the website thus may be easier and more productive. Cookie files are important. Without them, web browsing would be much more complicated.

Legitimate interest
Interest of the controller or a third party for example in a situation when the data subject is a customer of the controller, however with the exception of cases when interests of the subject or his/her fundamental rights and freedoms prevail over these interests.

Personal data

Information on a specific, identifiable person.

Recipient

Person to whom data are delivered.

Service

Any of the services that we offer to you, including our products, services offered online and their promotion.

Controller

Entity which determines the purpose and means of the processing of personal data; the controller may authorise a processor to do the processing.

Data subject

Living person to whom personal data relate.

Purpose

Reason for which the controller uses your personal data.

Goods

Product that you buy from us, typically a car, but also an application for your mobile phone.

Processing

Activity that the controller or the processor do with personal data.

Processor

Entity processing personal data for the controller.

15. CATEGORIES OF PERSONAL DATA

Below you will find individual categories of personal data and a breakdown of specific data included in them.

Identification data:

Name, surname, maiden name, pre-nominal letters/post-nominal letters, gender, language, domicile, permanent residence, date and place of birth, data of death, citizenship/nationality, person identifier (allocated by the company), type of the document, number of diplomatic passport, number of identity card, corporate ID, tax ID, social security number, number of the driving licence, passport number, expiry date of the document, data and place of document issuance, photograph from the identity card,

log-in in the application, date of origination/cancellation of the record, employee number, employer, job position, number of press credentials, signature.

Contact information:

Correspondence address, work place address, telephone number, fax number, email address, data box, contact information in social media.

Psychological characteristics:

Any information on the character/personality/state of mind/mood.

Physical characteristics:

Any physical characteristics (colour of hair, eyes, height, weight, etc.).

Risk profiles:

Cyber risk, AML risk, fraud risk, CFT risk, embargo risk, PEP, other safety or security risk.

Information on family and other persons:

Marriage, partnership, marital status, number of children, information on the household, name and surname of a child, date of birth of a child, information on another person (kinships and other relationships).

Descriptive data:

Social status (student/employee/self-employed/person without income), job functions and work experience, skills, education, qualifications, lifestyle, habits, leisure time and travelling, membership for example in charity or volunteering organisations, information on the area where the data subject lives, information on housing, important moments in lives of subjects (relocation, obtaining of a driving licence), health insurer code, firearms licence (yes/no), left-handed/ right-handed, number of the EHIC, preferred dealer, copy of the sick leave document, segmentation.

Copy of the personal identity card or another public document:

Copy of the identity card, copy of the passport, copy of the seriously disabled person card or the seriously disabled person with a companion card, copy of the driving licence, copy of the diplomatic passport, copy of MOT, birth number.

Information on race or ethnic origin:

Race or ethnic origin.

Political views:

Political views.

Information on religion or philosophical beliefs:

Religion or philosophical beliefs.

Information on membership in trade unions:

Membership in trade unions. Genetic data: genetic data.

Biometric data:

Biometric data (signature, photograph).

Information on rulings in criminal matters and criminal acts or relating safety and security measures:

Information relating to rulings in criminal matters and criminal acts or relating safety and security measures.

Health data:

Physical health, mental health, risk situations and risk behaviour, seriously disabled person, seriously disabled person with a companion, blood type, information on healthcare, information on sex life or sexual orientation.

Salary and similar data:

Salary/remuneration, salary compensation, average earning, bonuses/use of benefits, deductions from salary, manner of sending of salary, expenses, private account number, use of internal sources, insurance, taxes and deductions, statement of a taxpayer, tax returns and underlying documents, information on the assets of an employee.

CVs, cover letters and records from recruitment processes:

CVs, cover letter, records and results from recruitment processes.

Information on work:

Job position, cost centre, senior employee, working hours & national holiday, vacation, sick leave, maternity/parent leave, career break, presence, events, calendar, home office, teleworking, information on business trips and other changes in employment, daily programme/timesheets, entrusted devices and other valuables, ICT assets, number of worked hours, completed trainings, access rights, log of work-related injuries, work for a third party, received and made donations.

Evaluation and relating communication:

Feedback from employees, responses in surveys, complaints/suggestions/proposals/requests/questions and dealing with them, servicing requirements, evaluation records, internal sanctions, self-evaluation, personal goals and KPIs.

Other identification and contact information of an employee:

Employee card number, user ID, work email accounts, work telephone number, passwords in internal IT systems, access/logs to internal IT systems – VPN connection, information on employees from the group.

Transaction data:

Bank account number, debit/credit card number, authorisations/powers of attorney, transaction dates, transaction amounts.

Trading history:

Transactions and contracts including relating information, offers/demands of business opportunities, subject matter, date, place of the transaction, reminders, information on trading in the group.

Business profile:

Business profile derived from analytical modelling, VIP and similar designation, intent to buy a car (when, what and financing) interest in test drive, solvency.

Information on internal control and investigation:

Records from internal investigation, whistleblowing cases, internal system logs, logs relating to internet use/operations, logs relating to the use of email services/operations, logs relating to the use of telecommunications means/operations.

Records from CCTV systems:

Records from CCTV systems.

Records from input devices:

Records from input devices.

Information on movement on the premises:

Information in the guest book.

Photographs/video:

Photographs, video.

Voice recordings:

Voice recordings.

Communication, interactions and profiles derived from these data:

Chat (instant messaging), conversations, email communication, behaviour or browsing/clicking /search and listening/ browsing relating to internet/emails/media/applications, information obtained through

feedback/surveys/ comments/suggestions/complaints relating to the controller, approval / disapproval of the type of form of communication.

Localisation data:

Localisation data based on GPS localisation data derived from other operations (e.g. card payments to the trader on the business premises).

Network identifiers:

Mac address, IP address, Device Fingerprint, cookies or similar browser information technology.

Information on the course of studies:

Form, field of study, marks, student evaluation, work experience.