WHAT MUST BE TAKEN INTO ACCOUNT WHEN PERSONAL DATA IS STORED AND USED?

An important goal of data protection is to prevent the misuse of personal data. If unsecure IT systems are tampered with, criminals can intercept bank data and thereby gain unauthorized access to accounts. They can use personnel numbers or IDs to create and sell fake documents. Misuse of personal data often has a financial reason. This makes it that much more important to handle data in compliance with data protection laws. In other words, we must obligate our employees to uphold data secrecy, regularly equip our IT systems with the latest security software, send data only over encrypted channels and secure our computers as well as diagnostic devices against unauthorized access by means of password protection. Additionally, we must keep data that is in paper form in suitable lock boxes and delete personal data when the purpose for its collection no longer exists. These are some of the most important specifications from the law to guarantee data security.

To protect your data against hacker attacks, Hella Gutmann Solutions GmbH uses suitable encryption programs to transmit data through the diagnostic device. In the future, you will also be able to use a password function for the diagnostic device.

WHAT ARE THE POSSIBLE FINES FOR NON-COMPLIANCE WITH THE REGULATIONS?

The maximum fine is 20 million euros, or up to 4 % of total annual sales gained worldwide in the preceding fiscal year, depending on which value is higher. Of course, such amounts are far removed from the reality of a medium-sized workshop, but they are also only the most severe penalty for failure to comply with the legal provisions. Experts anticipate that the new fines will start at around 30,000 euros, which is already enough to be quite painful.

STARTING ON MAY 25, 2018, THE NEW EU GENERAL DATA PROTECTION REGULATION GOES INTO EFFECT

TO RECAP EVERYTHING BRIEFLY

INDISCRIMINATE STORAGE OF CUSTOMER OR EMPLOYEE DATA IS PROHIBITED.

We need personal data for many situations in everyday work, such as the customer's name to fulfill a contract, the VIN to read out vehicle data or the account data of an employee to transfer his or her salary. All of this data is the property of the corresponding persons. We are allowed to use it only to fulfill our legal obligations and to protect our business purposes, or if the owner has agreed to the use. Otherwise, no personal data is allowed to be stored or used.

DATA FROM CUSTOMERS OR EMPLOYEES IS ONLY BORROWED.

If we store personal data, we have to know at all times where the information is and what is being done with it. Because the data is only borrowed. Every customer and employee has the right to learn what data we have about him or her.
In addition, the data owners can demand to have their data back or have us delete it, if there are no legal grounds to the contrary.

EXERCISE CAUTION WHEN COMMUNICATING PERSONAL DATA.

Collected data is used solely within the company in very few cases. Frequently, for example, the tax consultant takes over payroll accounting, or the IT systems in use automatically save data to a cloud. When we use such services, we communicate personal data to third parties. This communication is permitted by law only to fulfill contractual obligations. At the same time, we are obligated to inform our customers or employees about this in such cases and to conclude an order processing contract with the corresponding service provider. If we want to transfer personal data for other purposes in addition, we need the data owner's consent.

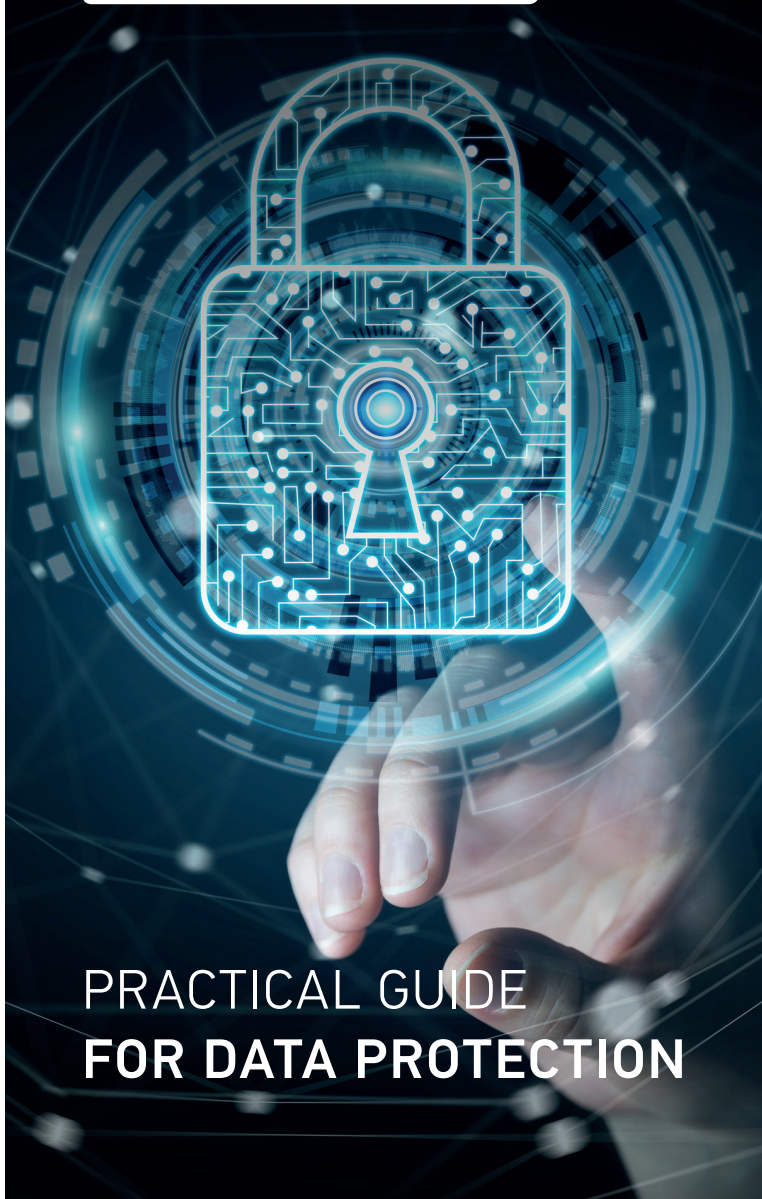
SECURITY IS FIRST AND FOREMOST.

When we are entrusted with personal data, we must handle it very carefully. Therefore, all data is to be kept in a way that does not allow any unauthorized access to it. This also means that we regularly equip our computers with the latest security software and log out when we are not using the computer or diagnostic device.

HELLA GUTMANN SOLUTIONS GMBH
Am Krebsbach 2 | D-79241 Ihringen, Germany | Phone: +49 7668-9900-0
E-mail: datenschutz@hella-gutmann.com | **www.hella-gutmann.com**

HELLA GUTMANN SOLUTIONS

IMPORTANT TIPS
TO KEEP YOU INFORMED



PRACTICAL GUIDE
FOR DATA PROTECTION

You have received this informational brochure because of the new EU General Data Protection Regulation, which takes effect as of May 25, 2018. The provisions in the legislation frequently use cumbersome language that, in many cases, is difficult to read and understand. That is why we have summarized some of the most important provisions for you in everyday language.

First, it is important for us to point out that data protection always concerns only PERSONAL data. This means that the only relevant data is data which can be used to identify a particular person. This includes both data that refers directly to a person, such as a name, address, or phone number, and data that allows for a person to be inferred with the help of additional knowledge. For example, this includes a personnel number, registration number or VIN.

TYPICAL PERSONAL DATA OF EMPLOYEES:

- Name, address
- E-mail, phone number
- Personnel number
- Bank details
- Health-related information
- Application documents

TYPICAL PERSONAL DATA OF WORKSHOP CUSTOMERS:

- Name, address
- Phone number, e-mail
- Credit card information
- Driver's license
- Registration number, VIN

AVOID HIGH FINES AND DISAPPOINTED CUSTOMERS

The new EU General Data Protection Regulation does not prohibit personal data from being collected and processed, but rather prescribes how we are to handle this data. About 80 % of the data protection regulations are already in effect. However, very few people know what is allowed and what is not. This is precisely where we would like to shed some light in this brochure.

WHEN ARE WE ALLOWED TO STORE AND USE PERSONAL DATA?

In everyday work, there are various situations in which we must be allowed to process personal data. For example, when we bill a customer for service or a repair, we need the name and address of the customer. We also need to see the driver's license before we can give the customer a rental car. We need the VIN to select the correct vehicle. And to be able to pay our employees their salary, we need their account data. If storage and processing of this data were prohibited, we would not be able to fulfill our contractual obligations or pursue our business purpose. But to enable us to do that, legislation permits storage and use of personal data for such purposes. However, we are required to keep a record of which personal data we have and what we use it for.

On the other hand, if we would like to store and use personal data for other purposes, we need permission from the customer or employee. For example, if we use the phone numbers of our customers to inform them about offers, we need their permission to do so. This also applies if we store data about their family environment to achieve better proximity to the customer. It is advisable always to obtain permission in writing, so that it can be proven. We should never ask for particularly sensitive data, such as political or religious beliefs or the genetic predisposition of our employees or customers. There are only very few cases in which this information is truly necessary. And these cases are virtually never found in workshops. We can follow the guiding principle that personal data is allowed to be collected and processed only if we need it for a substantive and relevant purpose.

WHO IS THE OWNER OF THE DATA?

The EU General Data Protection Regulation clearly states that each EU citizen is the owner of all of his or her data. This means that the personal data we collect and use is only borrowed. Every EU citizen has the right to learn what data we have about him or her and what we use this data for. Therefore, if he or she asks for information, we are obligated to provide it. In addition, every EU citizen can demand to have his or her data back or have us delete it, if there are no legal grounds to the contrary. If we have permission from a customer or employee to use his or her personal data, he or she can revoke this permission at any time. Here, too, we are obligated to satisfy this request. If we transfer personal data to a third party to fulfill our contractual obligations, we are obligated to inform the data owner of the purpose and extent of such transfer.

WHAT MUST BE OBSERVED WHEN TRANSFERRING PERSONAL DATA TO A THIRD PARTY?

Collected data is used solely within the company in very few cases. For example, if we send employee data to the tax consultant for payroll accounting, or if our IT systems (IT solution, diagnostic device) automatically save data to a cloud, we are transferring data to a third party. When doing so, the following four points must be observed.

- **First:** Personal data is allowed to be transferred without permission from its owner only to fulfill contractual obligations. For example, this means that if we have made an agreement with the customer to repair a car and need a diagnostic device to do so, we do not need the customer's permission in this case because we have to use the diagnostic device to carry out the repair and fulfill the contract. The repair would otherwise not be possible. Permission does not have to be granted separately for such cases.

- **Second:** In such a case, the data owner must be informed about this once.
- **Third:** We must conclude an order processing contract with the external service provider to ensure that the company handles the entrusted data in compliance with data protection laws.
- **Fourth:** If we want to transfer personal data for other purposes in addition, we need the data owner's consent.

ORDER PROCESSING CONTRACT.

If we communicate personal data to other companies, the law defines us as the **data controller.** The other company, on the other hand, is the **data processor.** As the data controller, we have to make sure that the data processor processes the communicated data correctly. This is guaranteed by an order processing contract, which has to be concluded between the data controller and the data processor. This contract should include a list of all the purposes of the data transfer. In addition, the technical and organizational measures of the data processor have to be attached to the contract as an appendix and describe the measures for fulfilling the security and protection requirements.

If a diagnostic device or exhaust gas analyzer from Hella Gutmann is used in your workshop, you have to conclude an order processing contract with Hella Gutmann Solutions GmbH.

To save you the task of creating such a contract, we have written this for you. The order processing contract is included in the attachment to this e-mail or can be downloaded from the homepage **www.hella-gutmann.com/privacy**. You only need to insert the company name of your workshop and send the signed contract to **av-vertrag@hella-gutmann.com**. An order processing contract must also be concluded with all other companies to which the personal data is communicated.