fleetcompetence Group Data Privacy Policy

To the Attention of: Cooperation Partner of fleetcompetence Group

1. SCOPE

1.1. GENERAL

The European General Data Privacy Regulation (EU GDPR) gets into force on May 25. It stipulates increasing requirements with regard to data privacy. This Data Privacy Policy has been set up to cover the requirements with regard to the cooperation between fleetcompetence international GmbH and its international Partner.

The GDPR regulates data protection. However, it is not around any data, but specifically around the so-called **personal data**. According to Article 4 (1) EU GDPR **'personal data'** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

All following formulations and definitions are in accordance with the EU GDPR, especially with the definitions of Article 4 EU GDPR.

1.2. APPLICABILITY

This Policy applies to fleetcompetence international GmbH, Switzerland, and all Partner with whom fleetcompetence international has signed a Cooperation Agreement, jointly hereinafter named fleetcompetence Group.

This Policy is applicable regarding the data privacy requirements for the execution of projects of fleetcompetence international, jointly together with their Partner.

This policy only applies in the context of fleetcompetence's projects and is not binding for any other operations, anyhow it's recommended. Any regulation targeting a device or the general protection of a device as access point to personal data entrusted to fleetcompetence, the regulation applies permanently, independent whether the device is at this time used for a fleetcompetence project or not. The scope overarches therefore all participating people independent of their contract type (i.e. regular employee, freelancer, …).

1.3. PARTNERS RESPONSIBILITY

This Policy is not covering all legal obligations regarding the European General Data Privacy Regulation (EU GDPR). These must be implemented by each Partner regarding his own organisation.

This regulation especially does not cover the following data privacy areas; however, it's expected that all of these areas are compliant with the EU GDPR:

- Data privacy officer
- Processes for data subjects
- Data privacy for employees
- Data processing contracts
- General data privacy process list
- Audits of subcontractors
- Marketing
- Website
- Education of employees
- Management of documents

2. RESPONSIBILITY REDUCTION

Each partner can reduce the responsibility by agreeing to exclusively using fleetcompetence's IT solutions in certain areas (only applying to fleetcompetence projects), which exempts the partner from the responsibility to implement the above mentioned regulations *marked in green and italic font*.

The following areas are covered by fleetcompetence and have to be used exclusively for

- E-Mail (for all kind of written communication)
- Cloud (for all kind of file transfers)

If the above mentioned IT solutions are used, then the partner has to ensure that all project files on local devices are not backed up in the company network. It's also prohibited to automatically forward mails to an external mail or to synchronize the cloud files with another cloud.

3. REGULATIONS

3.1. ORGANIZATION AND STAFF

3.1.1. ORGANIZATION

- *There has to be a clear concept which employee has access to which kind of data.*
- External visitors have to be accompanied permanently by an employee.
- *Employees only have access to files they need, not to files they might need someday.*

3.1.2. STAFF

- *There has to be a clear introduction concept for new employees explaining all data privacy relevant rules and procedures.*
- *There has to be a clear concept for the IT procedures if an employee leaves the company.*
- *There has to be a replacement rule to ensure that process critical employees have always a replacement.*
- All internal and external employees have so sign a NDA.

3.1.3. SENSITIZATION AND EDUCATION

- *There has to be a data privacy sensitization for every project lead.*
- There has to be a nominated data security and privacy coordinator.
- There has to be an introduction for every IT software covering the data privacy risks if they are not designed data privacy friendly by default.

3.1.4. IDENTITY AND ACCESS MANAGEMENT

- *There has to be a clear rule for the user (group) management.*
- *There has to be a clear rule for granting, modifying or withdrawing permissions.*
- *There has to be a list of users and their permissions, which get re-evaluation regularly.*
- *There has to be a clear definition of responsibilities and which permission each responsibility requires.*
- There has to be a password rule ensuring a minimum length and complexity of passwords according the current technical standard.
- *Every IT system containing personal data has to be protected with an identification system.*
- Sharing an account with another person, even temporarily, is strictly prohibited.

3.1.5. COMPLIANCY MANAGEMENT

- As a rule, no personal data shall be requested or received from Clients in the course of a project.
- In case, personal data are necessary for the purpose of a project, the project manager has to ensure that only personal data are requested, which are needed for the execution of the project.
- There have to be regular audits of the proper implementation of this regulation’s rules.

3.1.6. DATA PRIVACY FRIENDLY DATA COLLECTION

- The collection of personal data is only permitted, if it’s necessary for the work.
- Personal data, which is not needed anymore, has to be deleted immediately (including backups).

3.2. CONCEPTS AND PROCEDURES

3.2.1. CRYPTOGRAPHY

- Every device containing personal data has to be encrypted with a proper cryptographic algorithm using recommended key lengths according current technical standards.
- Cryptographic keys have to be stored securely to ensure a decryption is always possible.
- All written communication has to be transferred in an encrypted way (i.e. SSL/TLS).

3.2.2. BACKUP CONCEPT

- *There has to be a concept defining which data are backed up in which interval.*
- *There has to be a blocklist for personal data, which is not allowed to be restored.*

3.2.3. SELECTION AND USAGE OF STANDARD SOFTWARE

- The integrity of standard software has to be validated (i.e. hash comparison).
- Software, which violates the rules stated in this document, is not permitted.
- The software has to be updated regularly.

3.2.4. DELETION

- *There have to be clear rules for the deletion of files preventing the mistaken deletion of files as well as ensuring a safe and intentional deletion.*

3.2.5. INFORMATION SECURITY DURING BUSINESS TRIPS

- All travelling employees have to be educated about the increased security risks during business trips.
- All devices have to lock automatically after a certain inactivity time.
- A VPN has to be used if an employee uses any other network than the company’s network.
- All on business trips used devices have to be encrypted.

3.3. OPERATIONS

3.3.1. IT ADMINISTRATION

- *Only qualified people are allowed to do the IT administration.*
- *The IT administrators have to be reliable and careful.*
- *There have to be replacements for each critical IT administrator.*
- *Every IT administrator has to have an own, unique identification.*
- *Every administrator password has to be different, even for different systems of one administrator.*

3.3.2. UPDATE AND CHANGE MANAGEMENT

- *Before each update a backup has to be done if the system contains personal data.*
- *All users of the IT system have to be informed 24h before the update/change.*

- *There have to be clear responsibilities who is responsible for which update.*

3.3.3. MALICIOUS SOFTWARE PROTECTION

- Every device containing personal data has to have an anti virus program.
- Every software (including anti virus programs) have to be updated regularly.
- *Every gateway device (i.e. mail servers) has to have an anti virus program.*

3.3.4. ARCHIVES

- *There has to be an archive system for all personal data.*
- *There has to be software list for all archived files to ensure the accessibility in future.*
- *There have to be regular backups of the archives.*
- *All files in the archive containing personal data have to be deleted or at least pseudonymized after the project is completed.*

3.3.5. INFORMATION AND DATA MEDIUM EXCHANGE

- *There has to be a list of permitted communication channels.*
- *There has to be a rule which data are allowed to be exchanged via which communication channel.*
- Every lost data medium has to be reported to the data security and privacy coordinator.

3.3.6. REMOTE WORK

- All work has to be done on company devices.
- If company devices are used privately, there have to be technical measures to separate the private and business data.
- Data, which is not clearly declared as private data, is considered as business data.
- The rules for business trips apply except the employee works in an enclosed space dedicated to his work.

3.3.7. OUTSOURCING

- Using a processor always requires the permission of fleetcompetence.
- The processor has to comply with all regulations made in this document.
- *The processor has to receive separate authorization accounts.*
- *Using software as a service (SAAS)/cloud based services is also outsourcing.*

3.3.8. REMOTE MAINTENANCE

- Unmonitored remote maintenance is prohibited.
- The remote maintenance service has to be protected properly with authentication and encryption.
- If an external company executes remote maintenance services, then the outsourcing rules apply.

3.4. DETECTION AND REACTION

- A security relevant event is any event, which might lead to any breach of personal data.
- Detection of security relevant events
  - There has to be a clear system to detect security relevant events.
  - All security relevant events have to be reported to the data security and privacy coordinator.
  - *It has to be ensured that all legal boundaries are kept while log files are evaluated.*
  - *If IT systems have security features, these security features have to be activated.*
- Handling of security relevant events
  - All security relevant events have to be reported to the data security and privacy coordinator.
  - Company's data security and privacy coordinator has to create an impact, scope and risk analysis for each incident and inform fleetcompetence about the result.

3.5. APPLICATIONS

3.5.1. APPLICATIONS

- The integrity of each software has to be ensured (original and unchanged software).
- The automatic execution of interactive content (i.e. Active X or Flash) has to be disabled.
- All external files have to be scanned for malicious content before they are opened.
- All available security patches have to be installed.
- The automatic update check has to be enabled.

3.5.2. WEB APPLICATIONS

- *All web applications, containing client's personal data, out of the company network have to provide an encrypted connection (SSL/TLS via https); a browser plugin to always check the availability of encrypted connections is recommended.*
- *Every web application has to be secured by an authentication system.*
- *All available security patches have to be installed.*

3.6. NETWORKS AND COMMUNICATION

- Every wifi has to be encrypted with common encryption standards, WPS is prohibited.
- Guest networks have to logically separated from the operational company network.
- The usage of any not by your company controlled network is only permitted with encrypted connections.

3.7. INFRASTRUCTURE

- The physical access to all devices has to be restricted/controlled.
- This restriction also applies for home offices.

4. EXAMPLES

The following list showcases the implications for the daily working life, however this list is just exemplary and not concluding:

- Personal data are not allowed to be sent via e-mail as it is not possible to ensure a static encryption between all email servers. The cloud has to be used to transfer the file.
- Sharing a whole client folder with everyone, who’s working on parts might not be permitted. A client folder should always be separated in projects and employees have only access to the project they work on.
- One computer is used by several employees, so each employee needs to have an own account, a shared login for all employees is not permitted.
- For a fleet scan it’s normally not permitted to receive the drivers’ names as VIN number or number plate (only if there is no public database) is normally enough for a unique identification of the car.
- “Lending” a colleague your credentials to quickly download something is prohibited.
- After the completion of a project all data should be reviewed, personal data deleted (if not needed for legal documentation) and all other data archived.
- Using you private computer, for which one of your relatives has the administrator password, is prohibited.

5. EXCEPTIONS

Exceptions can be granted by fleetcompetence’s data security and privacy coordinator if the partner can proof, that a lower standard will not risk the client’s personal data or the preventive measure represents an unreasonable effort for the partner compared to the risk for the client’s personal data.