Data Processing Agreement

In accordance with the European Parliament- and Council's Directive (EU) 2016/679 of 27th April 2016 (hereinafter GDPR) on the protection of physical persons in connection with the processing of personal data and on free

exchange of such information, Articles 28 and 29, cf. Articles 32-36, the following agreement is concluded

between

ColliCare Logistics

....

Data Controller

and

(system supplier)

....

Data Processor

1. Purpose of the Agreement

To regulate the rights and obligations under the GDPR on the protection of physical persons in connection with the processing of personal data and on the free exchange of such information.

The agreement is intended to ensure that personal data is not used illegally, wrongfully, nor that information is processed in ways resulting in unauthorized access, alteration, deletion, damage, loss, or unavailability.

The agreement governs the Data Processor's management of personal data on behalf of the Data Controller. It includes collection, registration, compilation, storage, disclosure or combination of these, in connection with the conduct of transport- and logistics services and administrative services within the company, like salary and personnel.

In the event of conflict, the terms of this agreement shall precede the Data Processor's personal privacy declaration or the terms of any other agreements entered into between the Data Controller and the Data Processor in connection with the conduct of transport- and logistics services.

2. Instructions

The Data Processor will follow the written instructions for the management of personal data which the Data Controller has determined should apply.

ColliCare Logistics is obliged to abide by all obligations under the GDPR that apply to the processing of personal data in the conduct of transport- and logistics services.

The Data Processor undertakes to notify the Data Controller if it receives instructions from the Data Controller that violate the provisions of GDPR.

3. Purpose Limitations

The purpose of the Data Processor's management of personal data on behalf of the Data Controller is to provide and manage transport- and logistics services and administrative services within the company.

Personal data that the Data Processor manages on behalf of the Data Controller may not be used for purposes other than delivery and administration of transport- and logistics services, and administrative services within the company, like salary and personnel, without prior approval of the Data Controller. The Data Processor is not permitted to transfer personal data covered by this agreement to partners or other third parties without prior approval of the Data Controller, cf. point 10 of this agreement.

4. Types of information and registered persons

The Data Processor manages personal data on behalf of the Data Controller in connection with the delivery and management of transport- and logistics services. Data can be;

- name and surname
- home address

- an email address such as name.surname@company.co
- social security number
- phone number

5. The rights of registered persons

Data Processor is responsible for assisting the Data Controller in safeguarding the rights of the registered person, cf. GDPR, Chapter III, Articles 13 to 23.

The registered person's rights include the right to information about how his or her personal data is processed, the right to request access to their own personal data, the right to request corrections or deletion of their own personal data and the right to require that the processing of their personal data be limited.

To the extent relevant, the Data Processor will assist the Data Controller in maintaining the registered person's right to data portability and the right to oppose automatic decisions, including profiling.

The Data Processor is liable for damages to the registered person if errors or omissions on the part of the Data Processor inflict financial or non-financial loss on the registered person as a result of their rights or privacy protection being infringed.

6. Satisfactory information security

The Data Processor will implement satisfactory technical, physical and organizational safeguards to protect personal data covered by this agreement from unauthorized or unlawful access, alteration, deletion, damage, loss, or unavailability.

The Data Processor will document its own security organization, guidelines and routines for security work, risk assessments and established technical, physical or organizational safeguards. The documentation should be available to the Data Controller.

The Data Processor will establish continuity- and contingency plans for effective handling of serious security incidents. The documentation should be available to the Data Controller.

The Data Processor will provide its own staff with sufficient information on, and training in, information security to ensure that the security of personal data managed on behalf of the Data Controller is taken care of.

The Data Processor will document the training of its own staff in information security. The documentation should be available to the Data Controller.

7. Duty of confidentiality

Only employees of the Data Processor, who have a work-related need to access personal data that are managed on behalf of the Data Controller, may be granted such access. The Data Processor is required to document access management guidelines and routines. The documentation should be available to the Data Controller.

Employees of the Data Processor have a duty of confidentiality in respect of documentation and personal data which they obtain access in accordance with this agreement. This provision also

applies after the termination of the agreement. The duty of confidentiality includes employees of third parties performing maintenance (or similar tasks) of systems, equipment, networks or buildings used by the Data Processor to deliver or administer transport- and logistics services.

8. Access to security documentation

Data Processor is obliged to provide the Data Controller with access to all security documentation necessary for the Data Controller to be able to fulfil its obligations in accordance with GDPR, Article 5 No.1 letter f and Articles 32-36. The Data Processor is obliged to provide Data Controller with access to other relevant documentation that allows the Data Controller to evaluate whether the Data Processor is complying with the terms of this agreement.

Employees of the Data Processor have a duty of confidentiality in respect of confidential security documentation that the Data Processor makes available to the Data Controller.

9. Security breach notification

The Data Processor must notify the Data Controller without unreasonable delay if personal data that is managed on behalf of the Data Controller is exposed to any breach of security that involves the risk of infringement of the registered party's personal privacy.

The notification to the Data Controller should at a minimum include information that describes the security breach, which registered parties are affected by the security breach and what personal data is affected by the security breach. It should also state what immediate measures have been Implemented to address the security breach, and any preventive actions that may have been taken to avoid similar incidents in the future.

The Data Controller is responsible for ensuring that notifications of security breaches from the Data Processor are reported to the Norwegian Data Inspection Authority.

10. Subcontractors

The Data Processor is obliged to enter into its own agreements with subcontractors of transport- and logistics services that govern the subcontractor's management of personal data in connection with the delivery and administration of transport- and logistics services.

In agreements between the Data Processor and its subcontractors, the subcontractors are required to comply with all obligations to which the Data Processor itself is subject under this agreement. The Data Processor is obliged to submit the agreements to the Data Controller upon request.

The Data Processor will ensure that the subcontractors of the transport- and logistics services comply with their contractual obligations, in particular that information security is satisfactory and that employees of the subcontractors are aware of their obligations and fulfil these.

The Data Controller grants its approval to the Data Processor hiring the following subcontractors in connection with the delivery and management of transport- and logistics services.

The Data Processor is liable for damages to the Data Controller for any financial loss that is inflicted on the Data Controller and that is due to illegal or improper treatment of personal data, or inadequate information security on the part of subcontractors for transport- and logistics services.

11. Transfer to countries outside the EU/EEA

Background:

Personal data that the Data Processor manages on behalf of the Data Controller may be transferred to countries outside the EU/EEA (third countries). Such transfer may take place on certain terms, and the rules for transfer to third countries are to be found in Articles 45-47 and 49 of the Directive. These rules include, among other things, that the transfer will be lawful if it takes place to an EU-approved third country, to US companies in the United States who have joined the Privacy Shield scheme, or on the basis of the EU's standard contracts for the transfer of personal data to data processors in third countries. The rules also apply to backup and other transfer of connection with the administration of the relevant service, such as support.

Personal data that the Data Processor manages under this agreement may be transferred to other countries outside the EU/EEA when requested by our customers.

....

The legal basis for transfer of personal data to the aforementioned recipient countries outside the EU/EEA is

....

In order to conduct transport- and logistics services internationally, it is essential to be able to transfer the shipping information which may include the name of the contact person, e-mail address and telephone number.

12. Security audits and impact assessments

The Data Processor will regularly implement security audits of its own work with safeguarding personal data from unauthorized or unlawful access, alteration, deletion, damage, loss, or unavailability.

The Data Processor will enforce security audits of the information security in < name of service >. Security audits should include the Data Processor's security goals and security strategy, security organisation, guidelines and routines for security work, established technical, physical and organizational safeguards and the work of subcontractor information security to < name of service >. It should also include routines for notification to the Data Controller of security breaches, and routines for testing of emergency- and continuity plans.

The Data Processor should document the security audits. The Data Controller should be granted access to the audit reports. If an independent third party is conducting security audits at the Data Processor, the Data Controller should be informed of which auditor is being used and be granted access to summaries of the audit reports.

Data Processing Agreement

The Data Processor will assist the Data Controller if the use of transport- and logistics services means that the Data Controller is obliged to investigate the personal privacy impacts prior to the carrying out of the transport- and logistics services, cf. GDPR, Articles 35 and 36. The Data Processor can assist the Data Controller by implementing a personal privacy promoting action if the impact assessment shows that this is necessary.

13. Return and erasure

Upon termination of this agreement, the Data Processor is obliged to delete and return all personal data that is managed on behalf of the Data Controller in connection with the delivery and administration of transport- and logistics services. The Data Controller determines how the return of the personal data will take place, including the format to be used. The Data Processor will delete personal data from all storage media containing personal data that the Data Processor manages on behalf of the Data Controller. Erasure is to be done by the Data Processor transmitting the personal data within 30 days from the termination of the agreement. This also applies to the personal data backup.

The Data Processor will document that the erasure of personal data has been carried out in accordance with this agreement. The documentation should be made available to the Data Controller.

The Data Processor covers all costs associated with the return and erasure of any personal data covered by this agreement.

14. Breach of agreement

In the event of breach of the terms of this agreement caused by errors or omissions on the part of the Data Processor, the Data Controller may terminate the agreement with immediate effect. The Data Processor will continue to be obliged to return and erase personal data managed on behalf of the Data Controller pursuant to the provisions of point 13 above.

The Data Controller may claim compensation for financial loss, such as errors or omissions on the part of the Data Processor, including breach of the terms of this agreement, that is inflicted on the Data Controller, cf. also points 5 and 10 above.

15. Duration of the agreement

This agreement applies as long as the Data Processor manages the personal data on behalf of the Data Controller.

The agreement may be terminated by both parties with a 30 day mutual notice period.

16. Notices

Notices under this Agreement shall be sent in writing to:...

17. Choice of law and legal venue

The agreement is governed by Norwegian law as legal venue. (adjust to the country in question) This also applies after termination of the agreement.

This agreement is in two – 2 originals, one to each of the parties.

....

Place and date

On behalf of the Data Controller…………………………………….On behalf of the Data Processor

....

Signature)   Signature)

ColliCare Logistics