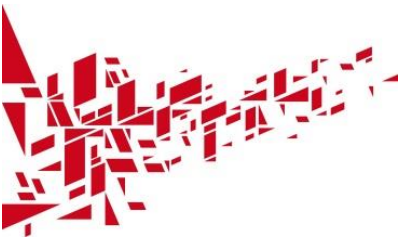


CONFIDENTIAL

AVIATION | DIVING | ENGINEERING & DEVELOPMENT | LIFTING & HANDLING | SUBSEA | WORKSHOP

General Data Protection Procedure



IM-A-ADM-KA-0015

General Data Protection Procedure

na	21/06/18	Issued for DIC	TVO	EA	GEO
Rev. No.	Date	Description	Originator	Checked	Approved
			IMENCO		

Document Title: General Data Protection Procedure

Imenco Procedure Number: IM-A-ADM-KA-0015

The screen version of the document is the "Controlled Copy" at all times.
When printed out it is considered a "For information only" copy, and it is the holder's responsibility that he/she holds the latest, valid version.

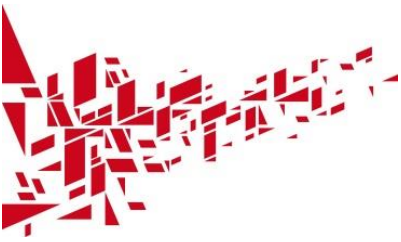


IM-A-ADM-KA-0015

Title: General Data Protection Procedure

Table of Contents

1	PURPOSE	4
2	SCOPE	4
3	RESPONSIBILITY AND AUTHORITY	4
4	DESCRIPTION OF ACTIVITIES AND EXECUTION	4
4.1	Implementation of the GDPR	4
4.2	Risk Analysis / Assessment	4
4.3	Approval	5
4.4	Collection / Data Transfer	5
4.5	Storage	5
4.6	Processing	5
4.7	Deletion	5
4.8	Breach of security	6
4.9	3rd parties	6
5	REFERENCES	7
6	APPENDICES	7



IM-A-ADM-KA-0015

1 Purpose

The purpose of this procedure is to ensure that the Imenco group handles personal data in compliance with Norwegian law "Lov om behandling av personopplysninger (personopplysningsloven)" LOV-2018-06-15-38 and the General Data Protection Regulation "GDPR" (EU) 2016/679

2 Scope

System(s) for protection of information relating to an identified or identifiable natural person.

3 Responsibility and Authority

The HR manager is responsible for implementing this procedure. The HR manager is authorized by signature to accept necessary cost of implementation.

The QA/HSE manger is responsible for creating and maintaining this procedure along with periodical compliance checking.

4 Description of Activities and Execution

4.1 Implementation of the GDPR

A groupwide survey of personal data shall be done to establish base line and ensure full compliance with the new regulation on form "Kartlegging av personopplysninger".

Existing but unnecessary data shall be permanently deleted, remaining personal data shall be summarized, categorized, risk assessed and data subject consent obtained.

4.2 Risk Analysis / Assessment

Before collection of new personal data is executed an assessment of:

- Legality
- Necessity
- Consequences of a security breach



IM-A-ADM-KA-0015

is carried out on form "Risikoanalyse"

4.3 Approval

Data Subjects are presented with a consent form which summarizes the personal information the company stores, it's intended use and period of storage.

4.4 Collection / Data Transfer

Collection and transfer of personal data is undertaken in a secure manner. Sensitive personal data is transferred through registered mail or secure connection / encrypted files if electronically transmitted. Methods include

- Direct transfer through a VPN tunnel
- Encrypted files
- Encrypted cloud transfers, i.e. Dropbox
- Encrypted USB stick

4.5 Storage

Personal data is stored in a secure manner.

Sensitive data is categorized, when necessary pseudonymized, and stored in encrypted folders with restricted access. Only personnel with legitimate needs have access to the specific folders.

Paper copies are stored in sealed envelopes in a locked filing cabinet, behind locked doors. Only the HR manager possesses the key.

Data subject may request access to his/hers personal data at any time using the form "Krav om innsyn i personalmappe"

4.6 Processing

Processing of personal data is only conducted as agreed with the data subject.

4.7 Deletion

Data is deleted upon data storage period expiry or when requested by the data subject within the confines of applicable laws and regulations



IM-A-ADM-KA-0015

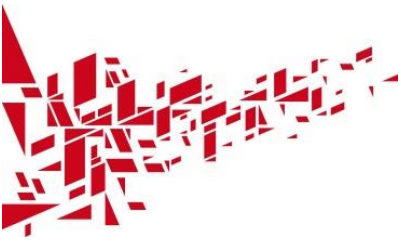
4.8 Breach of security

In the event of a security breach the user and the authorities are notified within 24h of the detected breach. The company will take immediate measures to limit the damages of the breach as far as practically possible.

Data security is continually monitored by contracted IT experts. The system is well tested and has worked without incident for several years.

4.9 3rd parties

Any third party that may access privileged personal data is required to sign a confidentiality agreement "Databehandleravtale"



IM-A-ADM-KA-0015

5 References

Lov om behandling av personopplysninger (personopplysningsloven)

General Data Protection Regulation

6 Appendices

Risikoanalyse

Samtykkeerklæring

Kartlegging av personopplysninger

Databehandleravtale

Krav om innsyn i personalmappe