1. General information:

1.1 Company information:

Company name:

Legal form:

Street name & number:

Postcode & place:

Country:

Telephone:

Email:

Website address:

Bank key:

Bank account:

Country code:

Account holder:

IBAN:

BIC:

Order address (if it deviates):

Group affiliation:

Subsidiaries/Locations:

Production sites:

VAT Identification Number:

Tax ID No.:

Year of founding:

Total number of employees:

Holdings in other companies (e.g. joint ventures):

The product groups/services which you offer:

1.2 Procurement information:

Order currency:

Payment terms:

Incoterms/Place of fulfilment:

1.8 Contact person:

Department:	Name:	Telephone:	Email:
Executive management:			
Sales:			
Procurement:			
Development:			
Production:			
Quality:			
IMDS Officer:			
Information Security Officer:			
Product Safety Officer			
Occupational Health and Safety Officer			

1.9 Financial data:

Annual turnover in the last 3 years (in EUR):

Year	Turnover
Year	Turnover
Year	Turnover

Investment volume in the last 3 years (in EUR):

Year	Volume
Year	Volume
Year	Volume

1.14 Code of conduct:

- We confirm receipt and implementation of the standardised rules described in the "Code of conduct for suppliers".

○ Yes ○ No

2. Questions regarding specific areas:

2.1 Quality:

Which standard is your QM system based on?   Valid until:
- ☐ IATF 16949 in the relevant valid edition
- ☐ Not existent but planned for next year
- ☐ DIN 9001 in the relevant valid edition
- ☐ Not existent but planned for next year
- ☐ Other certification:

(Please include a corresponding copy of the certification!)

2.3 Environmental management:

2.3.1 Environmental management system:

Which standard is your EM system based on?   Valid until:
- ☐ EMAS in the relevant valid edition
- ☐ ISO 14001 in the relevant valid edition
- ☐ Internal system, based on:
- ☐ Not existent but planned for next year

2.4 Occupational health and safety management:

Do you have an occupational health and safety management certificate?

Valid until:

- ☐ DIN ISO 45001 occupational health and safety in the relevant valid edition

- ☐ Not existent but planned for next year
- ☐ Other certification:

2.5 Energy management:

Do you have an energy management certificate?   Valid until:
- ☐ DIN 50001 energy management in the relevant valid edition
- ☐ Not existent but planned for next year
- ☐ Other certification:

2.6 Information security

<u>Has your ISMS been inspected by an independent body or do you have valid ISMS certification?</u>

<u>Valid until</u>

☐ ISO 27001 in the relevant valid edition
☐ TISAX
☐ Other

Please allow us to access your certificate electronically or provide us with your certificate.

If you do not have any of these certifications, please comment on the following statements.
(Note: Statements in bold have increased priority. If the answer to one of these statements or to 4 statements with normal priority is no, then an action plan will be required to enable us to exchange data with you!)

- **We have general guidelines for our employees which define our rules on information security.**

  ◯ Yes ◯ No

- We have guidelines which cover private use of our company IT.

  ◯ Yes ◯ No

- **We inspect our suppliers to confirm that they have implemented information security measures.**

  ◯ Yes ◯ No

- **All employees have signed a written non-disclosure agreement.**

  ◯ Yes ◯ No

- We have a strict rule that our IT infrastructure can only be accessed if this is necessary to carry out assigned duties.

  ◯ Yes ◯ No

- **Normal users are not given administrative access.**

  ◯ Yes ◯ No

- We review whether administrative access is necessary on a regular basis.

  ◯ Yes ◯ No

- **We provide our employees with training on information security issues on a regular basis.**

  ◯ Yes ◯ No

- Procedures for internal handling of confidential information have been defined in writing.

  ◯ Yes ◯ No

- We inform our users about the specific risks of mobile data carriers (e.g. that they can be lost or stolen or may be infected with malware) and increase their awareness of these risks.

  ◯ Yes ◯ No

- We have a protection concept to secure our IT systems.

  ◯ Yes ◯ No

- **We have a structured procedure defining how access to our company is given.**

  ◯ Yes ◯ No

- **We have structured visitor management which enables us to ensure that unauthorised persons cannot access data.**

  ◯ Yes ◯ No

- **We have a data backup system to protect ourselves against the loss of key company data.**

  ◯ Yes ◯ No

- **Current virus protection software is installed on our clients and servers.**

  ◯ Yes ◯ No

- We have guidelines which define how security incidents must be handled.

  ◯ Yes ◯ No

- **We keep our operating systems up to date (security updates, etc.).**

  ◯ Yes ◯ No

2.7 Audit rights

Will you grant us the possibility - if required - to carry out subsequent audits in your company?

Product audit
    If no, please specify reason:

◯ Yes ◯ No

Process audit
    If no, please specify reason:

◯ Yes ◯ No

Information Security Management System Audit:
    If no, please specify reason:

◯ Yes ◯ No

This document was completed by:

Name: _____   Email: _____

Place, date: _____   Signature, Company stamp: _____