Product Privacy, Security and Third-Party Information

Draft for approval. Do not use for binding orders or approved customer deliveries. Complete open fields before use; legal and commercial review is required.

1. Purpose and product identification

Use this accompanying document with the completed product schedule and actual release files. Product, version, delivery architecture and issue date [____]. It is not a certification or a guarantee of complete security. It makes no claims about unapproved functions or untested environments.

2. Data processing and roles

Shop and licence administration: Inceptum processes information needed for enquiries, orders, payment, licence assignment and statutory retention under the shop privacy notice. This includes the SAP system number and agreed licence scope. A system number is not a password, but should still be accessible only to authorised persons. Production data and credentials are not required as general licence evidence.

Product operation: responsibilities, storage locations and access depend on the actual deployment. In a customer-operated environment, the customer remains responsible for its business processing purposes. Installing software does not grant Inceptum or partners blanket permission to access data. Hosting or support on behalf of a customer is carried out only under an appropriate agreement and necessary data protection schedules.

3. Release-specific data flow record

Complete before delivery: data categories and purposes [____]; local and remote storage locations [____]; roles/permissions [____]; licence validation and any network connections [____]; telemetry/diagnostics and disabling options [____]; logs and retention periods [____]; optional external providers and countries [____]; legal bases/transfer safeguards [____]. Inactive features must be identified as such. An empty list does not establish absence of data processing.

4. Secure operation and reporting

The operator uses appropriate roles, protected connections, credential protection, current approved components and tested backup/restoration procedures. Changes are tested in a controlled manner. Vulnerabilities in ibSphere CRM may be reported confidentially to security@inceptumgroup.de. Include the product version, technical description and sanitised evidence, but do not send passwords or entire customer databases unsolicited. A suitable transfer channel for confidential details can be arranged.

The binding reporting channel for wizard must be confirmed before delivery. The completed product schedule states the support end date and update route. A security contact is not a general support SLA. Manufacturer assessments, including applicable CRA duties, are performed through the release process; these documents declare neither CE nor CRA conformity.

5. Third-party components and document versions

Each approved package includes the actual applicable Third-Party Notices and required licence texts; a generic template does not replace them. Where component licences require source code or a source-code offer, this must be provided for the release. The SBOM identifies components but does not replace licence texts. SAP and other trademarks belong to their respective owners; an integration description does not imply manufacturer partnership or certification.

Contract files are linked to the order by version and checksum. A new version accompanying an update does not automatically amend existing contracts. Changes with contractual effect require a valid agreement. Technical installation acknowledgements must be distinguished from the original evidence of contractual acceptance.