MEASURES

Datlinq has taken the following technical and organizational measures to adequately protect the data it processes against loss or any form of careless, incompetent or illegal use or processing in accordance with the ISO 27001 standard.

When desirable, you can request for our Statement of Applicability ISO 27001 via iso@datlinq.com

CONFIDENTIALITY

Physical access control
Protected and restricted access
Restrictions by means of a card key
Alarm system
Provisions on physical access control (manually / electronically)
Data processing systems are located in a closed area with restricted access
Definition of physical access authorizations for third parties
Manual locking systems
The data center in which the personal data are stored must be compliant with ISO 27001
Identity checks at the reception
Key regulation/key book/key issuing
Careful selection of the security staff/guard personnel
Video surveillance of the accesses
Careful selection of cleaning staff
Regular checking of the access records for abnormalities
System and data access control
Guidelines which govern the storage of back-up copies.
Authentication of the users by password/PIN (minimum length, use of special characters, etc.)
Authentication and/or recording of the devices
Use of anti-virus software
Use of firewalls (hardware, software)
Use of intrusion detection systems
Use of mobile device management
Locking of casing
Blocking of external interfaces (e.g. USB connections)
Certificate-based access authorization
Logging of accesses to critical data systems
Use of document shredders
Proper destruction/deletion of data carriers
Recording of the destruction of data
System-based authorization administration/identity management
Release/disclosure of data to authorized persons only
User administration (only entitled/authorized persons get basic access)
Password issuing/password rules (length, change etc.)
Guidelines for associates as well as training concerning the individual work processes and access authorizations to personal data
Number of administrators to be reduced to the “minimum” necessary
Elaboration of an authorization concept and release of data for authorized persons only
Data carrier administration including guidelines for storage
Effective and appropriate disciplinary measures against persons who access personal data without authorization

Transmission control
Use of adequate firewalls in order to secure the interfaces and lines through which the data are transmitted
Use of safe connections (e.g. encrypted/VPN)
Documentation of the recipients of data and the time of planned transfers for use and/or agreed deletion periods
Drafting of an overview of regular retrieval and transmission procedures
List of procedures
Recording measures
Pseudonymization
Strong access limits to information which reveal the actual data subject
Encryption
Encryption of (mobile) data carriers/removable media
Access through secured/encrypted connection only
Encryption of data carriers (according to industry standard)
Encrypted storage according to applicable industry standards

INTEGRITY

Entry/Input Control
Taking of access control measures, as described under 'System and data access control'
Measures for the protection from unauthorized changes and/or deletion of the stored data
Recording of the input, modification and deletion of data
User identification in accordance with access control
Recording of access to applications, in particular at the input, modification and deletion of data
Creation of an overview of applications with which data have been input, modified and deleted
Transparency of input, modification and deletion of data through individual user names (no user groups)
Issuing of rights to input, modify and delete data based on an authorization concept
Integrity control (detection of integrity violations)
Periodical check of integrity of data
Real time detection of integrity violations
Intrusion detection systems

AVAILABILITY

Availability control
Rules which prohibit the storage of personal data on local media
Fire-fighting equipment in server rooms of data centers
Infrastructure redundancy (e.g. load distribution, RAID, etc.)
Fire alarm and smoke detector systems (at data centers)
Equipment to monitor temperature in server rooms
Air-conditioning system in server rooms of data centers
Power socket strips in server rooms of data centers
Uninterruptable power supply (UPS) at data centers
Overvoltage protection at data centers
Anti-virus concept/malware protection
Storage of data back-up at a safe, external location
Regular data back-up in accordance with the back-up and recovery concept
Effective emergency plan
Server rooms not under sanitary facilities
Proactive monitoring of resources for bottlenecks or possible outage
Resilience control
Continuous performance monitoring and proactive solution of bottlenecks
Performance Testing during development and changes
Recoverability control
Regular back-up recovery check

PROCESS CONTROL AND EVALUATION OF EFFECTIVENESS

Contract/Job control
Access controls as under 'System and data access control'
Regular validation of access rights
Clear written instructions to the processor concerning the scope of processing of personal data. The scope is restricted to requirements to be met by the specific system development and database administration of Datlinq.
Securing of the destruction of data after the end of the contract
Securing compliance of the staff of the processor with data privacy
Contractual penalties for infringements
Prior check of the security measures taken by the processor and corresponding documentation
Separation control
Modules in the database of the processor distinguish the different purposes for which the data are used, e.g. differentiation by functionality and function
Interfaces, batch processing and reports are only configured for certain purposes and functions so that data collected for certain purposes can be processed separately
Physically separated storage on separate systems or data carriers
Separation between the productive and test system
Security measures ensuring that only authorized users can access the data
Separate databases
Security measures which ensure that only authorized users can access the data
Logical client separation (software side)
Elaboration of an authorization concept
Retention / deletion control
Rules for deletions
Data protection by default
Review of requirements with respect to implementation
Data Protection Management / Effectiveness controls / Certificates
Regular provisioning of security / data privacy certificates
Regular audit of supplier

SUB-PROCESSORS

The GDPR clearly sets out the rights and obligations of sub-processors and requires them to meet strong contractual requirements. Technical architectures in the cloud are complex and regularly involve several layers of data processors. When personal data is processed in the cloud, the GDPR (1) requires a high degree of transparency. Article 28(2) and (4) of the GDPR directly deal with the situation where a processor engages "another processor," which can be called a "sub-processor".
Datlinq is working with the following sub-processors:

IAAS

Name	Address	Area of use
TransIP	Schipholweg 9B 2316 XB Leiden Netherlands	Colocation / servers

PAAS

Name	Address	Area of use
Google Cloud Storage	1600 Amphitheatre Parkway Mountain View, CA 94043, USA	Cloud storage and processes, Data in EU Economic zone
Amazon web services	1200 12th Ave S, Ste 1200, Seattle, WA 98144, USA	Cloud storage and processes, Data in EU Economic zone (Frankfurt, Ireland)

SAAS

Name	Address	Area of use
ESRI	Weena 695 (B2.036) 3013 AM Rotterdam Netherlands	GIS application
Tableau	Blue Fin Building 110 Southwark Street London, SE1 0SU, UK	Dashboard application
Zendesk	30 Eastbourne Terrace Paddington London, W2 6LA, UK	Customer service software
Atlassian	Singel 236 1016 AB Amsterdam Netherlands	Software development (Bitbucket, Jira, Confluence)
Own Cloud	Rathsbergstraße 17 90411 Nürnberg Germany	Tool for secure data transferring
Sendgrid	41 Corsham St London, N1 6DR, UK	Mailhub for the purpose of Salesmapp
Zapier	548 Market St. #62411 San Francisco, CA 94104-5401, USA	API connector

Call Center

Name	Address	Area of use
GDCC	Conradstraat 18 3013 AP Rotterdam Netherlands	Call center

Marketing & Sales tooling

Name	Address	Area of use
MailChimp	675 Ponce de Leon Ave NE Suite 5000 Atlanta, GA 30308 USA	Emailing software EU-U.S. Privacy Shield