InfoVista Technical and Organizational Measures according to Art. 32 GDPR

Having taken into account

- the state of the art,
- the costs of implementation and
- the nature, scope,
- context and purposes of processing as well as
- the risk of varying likelihood and severity for the rights and freedoms of natural persons,

In our opinion, InfoVista has implemented appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

In assessing data security risk, consideration was given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

A. Measures for the assurance of confidentiality and integrity

1.	**Physical access control to the server rooms**
1.0	Personal data are stored in more than one server location / data center (i.e. on back up servers, cloud services).
1.1	Location of the server rooms operated by Infovista: Operated by Infovista: Massy (France), Kuala Lumpur (Malaysia), Gatineau (Quebec, Canada), Ashburn (Virginia, USA).
1.2	Location of the server rooms operated by sub-contractors: Telanox (India), Linkquest (India).
1.6	The server room are windowless.
1.8	The server room are secured by an alarm system.
1.9	The IT Director and Office Manager are informed if an alarm system is triggered.
1.10	The server rooms are not under video surveillance.
1.12	People who have access to the server rooms: Number of persons: up to 50 Role in the company: IT, R&D and customer support employees
1.13	There is an electronic lock system in place in the server rooms.
1.14	RFID and Company issued ID card entry technologies are in use.
1.15	Access rights are assigned individually.
1.16	Successful as well as unsuccessful attempts to access to the server rooms are logged in the access system.
1.17	Access data is stored for 90 days before erasure.
1.20	The server rooms are not being used for other purposes besides their actual function.
2.	**Physical access control to the office rooms**

2.1	Location(s) of the InfoVista workstations, from which personal data are accessed: Infovista offices: USA, Canada, France, UK, Sweden, Germany, Spain, UEA, Malaysia, India, Singapore, China, Japan, Australia.
2.2	There is a porter service during business hours in the lobby area to the building / to the office.
2.3	Visitor's book is implemented.
2.4	Visitors will be received at the entrance / reception by the contact person and must be accompanied at all times.
2.5	The building or the office is protected by a burglar alarm.
2.6	A commissioned security firm is informed if the alarm system is triggered.
2.7	The office building or its entrances are under video surveillance, with image recording.
2.8	The video footage is stored 90 days.
2.9	The building / office rooms are secured with an electronic lock system.
2.10	RFID entry technology is in use
2.11	Access rights are not assigned individually.
2.12	Successful as well as unsuccessful attempts to access to the building / office rooms are logged in the access system.
2.13	Access data is stored before deletion for 90 days.
2.14	The records are regularly assessed.
3	**Logic access control to the IT system**
3.1	Location(s) of the InfoVista workstations, from which personal data are accessed: Infovista offices (section 2.1) France, UK, Sweden, UEA, USA, Canada, Malaysia, India, Singapore, China, Japan, Australia.
3.2	There is a defined process for the distribution of access information (e.g. user names) and access rights for newly instated / removal of access information for departing employees, or for organizational changes.
3.3	Assigning or changing the access information is recorded in the MIS Helpdesk.
3.4	Employees log in via an individual authorization in the central directory service.
3.5	Single sign-on password parameters are in operation.
3.6	Password character length: 7 The password does not need to contain special characters. Expiration period in days: 90 days
3.7	The IT system enforces all users to comply with the above-mentioned password requirements.
3.8	There is by default an automatic screen lock after a defined length of inactivity (user may change this parameter).
3.9	When a password is lost, forgotten or compromised, admin issues a new initial password.
3.10	There is a limited amount of 6 unsuccessful log in attempts that can be made.

3.11	When the maximum number of unsuccessful attempts have been made, access will remain locked for 15 minutes
3.12	Authentication occurs for remote accesses by password. Multifactor authentication is required for remote access by admins.
3.13	There is a limited amount of 6 unsuccessful log in attempts that can be made.
3.14	When the maximum number of unsuccessful attempts have been made, access will remain locked for 15 minutes.
3.15	Remote access is disconnected after 15 minutes of inactivity.
3.16	The systems that process personal data is secured by a firewall.
3.17	The firewall is updated regularly and automatically.
3.18	Internal IT administer the firewall.
3.19	Successful and unsuccessful intrusions are recorded.
4	**Measures for the assurance of paper documents, mobile data carriers and mobile devices**
4.1	Redundant documents containing personal information (e.g. printouts / files / correspondence) are disposed of via wastepaper / residual waste.
4.2	Redundant data media containing personal information (e.g. hard disks) are disposed of by deletion of data with no overwrites.
4.3	Mobile data carriers are permitted (e.g. USB sticks).
4.6	. Personal data on mobile devices (smartphones) are encrypted with vendor default encryption.
4.7	Employees process personal data on their own private mobile data carriers and mobile devices (bring your own device).
5	**Measures for secure data transfer**
5.1	Data transfers are usually encrypted via https/TLS, FTPS or VPN
5.2	An external service provider administers the keys / certificates.
5.3	Data transfers are not documented
6	**Measures for pseudonymization**
6.1	No pseudonymization is undertaken

B. Measures for the assurance of availability

1.	**Server rooms**
1.1	The server room has a fireproof / fire-resisting access door.
1.2	The server room is fitted with smoke detectors.
1.3	The server room is connected to a fire alarm control panel.
1.4	The server room is fitted with a nitrogen extinguishing system
1.5	The access doors and external walls of the server rooms are made of fireproof panels and walls (e.g. F90).
1.6	The server room is air-conditioned.
1.7	The server room has an uninterruptible power supply (UPS).
1.8	The power supply to the server room is not also ensured via a diesel-powered generator.
1.9	The functionalities in 1.2, 1.3, 1.4, 1.6 and 1.7 are regularly tested.
2	**Backup- and emergency concepts, virus protection**
2.1	A centralized backup is in place in Massy.
2.2	Backup restoration is not periodically tested.
2.3	Backups for HR, Finance, Legal (server M), R&D (server Terre) servers in Massy are done daily.
2.4	Central backups are stored by a backup service provider (Antemeta) on servers at a separate location (France).
2.5	Local backups for USA, Canada and KL servers are stored on hard drives.
2.6	The backup storage location is in a separate fire area from the primary server.
2.7	Backups are not encrypted.
2.8	Users are responsible for software installation.
2.9	The IT systems technologically are protected from data loss / unauthorized data access, via an always updated virus protection and anti-spyware.
2.10	There is a centralized and automated process for virus protection and anti-spyware updates.
2.11	Internal IT is responsible for virus protection and anti-spyware.
3	**Network connection**
3.1	The company has a redundant internet connection
3.2	The individual locations of the company are connected via a redundant connection
3.3	Internal IT is responsible for the network connection of the company