TECHNICAL AND ORGANISATIONAL MEASURES

The Data Processor sets out below the technical and organisational measures that will ensure a level of security appropriate to the risk:

1 – Appointment of a Data Protection Officer (DPO)

Pursuant to Article 37 of the GDPR, the Data Processor has appointed Téva Boesch as its Data Protection Officer, due to his professional qualities and his specialist knowledge of the laws and practices on data protection.

The Data Controller may contact the DPO at the following address: dpo@m6.fr

The Data Processor shall ensure that, in carrying out his duties, the DPO:

- is properly involved, in a timely manner, in all questions relating to the protection of personal data
- Is not given instructions
- Is subject to professional secrecy rules or a confidentiality obligation, pursuant to EU law or the law of the Members States
- May not be relieved of his/her duties or penalised by the Data Controller or any sub-processors

A CISO within the M6 Group Audit and Risk Control Department is responsible for defining IT security policies, rules or action plans, supporting their deployment and checking their application and effectiveness,

A first technical team is dedicated to managing the networks, systems and IT security of hosting and a second team to securing the M6 Group for the networks and user workstations.

2 – Internal Documentation

The M6 Group has produced a number of internal documents that set out its guiding principles on information security and personal data protection, in particular under the GDPR. In this context, Mindbaz undertakes to append to its internal rules:

- An Information Systems Security Policy
- A group personal data protection policy
- A M6 group IT charter
- A charter for IT technicians

The M6 Group shall ensure that employees are made aware of all these documents before the GDPR enters into force and represents that they ensure a level of confidentiality and security that is consistent with the requirements of prevailing regulations.

3 – Employees and confidentiality

The Data Processor undertakes to ensure that all group employees, irrespective of their roles, duties and seniority:

- Are aware of all Internal Documentation;
- Apply the Internal Documentation to all scopes to which it is relevant and, more generally, in protecting the M6 Group against risks to the security of its information systems and access to personal data;

- Collaborate on a daily basis with those responsible for the security of the information systems with a view to managing risks
- Remain constantly vigilant to threats to the security of the information systems;
- Handle digital data and transfer it externally in strict compliance with prevailing regulations.

The undertakings apply to all scopes, organisations, business lines and group processes.

The M6 Group shall also ensure that these employees are aware of regulations on the protection of personal data, particularly through training and awareness-raising days and the introduction of an internal control tool.

3 – IT Security

M6 WEB undertakes to protect personal, private, confidential and sensitive data and the systems used to process, collect or transport such data. This section describes the actions used by M6 WEB to deliver on its undertaking.

Access logic of Mindbaz

- Secure transmission of usernames by email and single message with a limited lifespan is carried out following users' creation request
- Password complexity is consistent with the French Data Protection Authority's (CNIL) recommendations: minimum of 8 characters with a number, a capital letter, a lower case letter and a special character
- Passwords are renewed every 6 months for customers
- Account blocking is effective after 5 unsuccessful attempts. The account is unblocked upon request from customer services
- The creation of a new password by password loss mechanism is available

Technical access

- Direct access to the Mindbaz database is not allowed to customers, secure APIs allow exchanges to be conducted between the Mindbaz service and customers' servers
- Database accounts are reviewed annually and documented in terms of use and ownership
- Server access is reserved only for the ODISO operating team

Encryption

- Web communications (“https”) are encrypted for Users and API calls
- Exchanges of data export files are made with the SFTP protocol using accounts distinct from the web application
- Users’ passwords are encrypted with cryptographic hashing using a grain of salt.

Logging and monitoring

- The application allows the conservation of application traces of:
    - actions administrating Mindbaz accounts
    - data exports carried out through Mindbaz
    - user account authentications
- IT systems also have low-level technical traces

Managing vulnerabilities

- Intrusion tests of the “black box” (blind) and “grey box” type (with valid identifiers) are carried out regularly by a PASSI (Cybersecurity audit) service provider (selected by the ANSSI - The National Cybersecurity Agency of France) and result in patches
- A web security analysis tool is used to continuously analyse the quality of encryption and the correct use of Http headers.

Physical access

- The data centre has video surveillance, badge and biometric access control equipment, 24-hour security service, bays enclosed in cages under key. Regular access reviews are carried out at least once a year and open the departure of the administrators
- The M6 Group's premises are also equipped with video surveillance, access control by badge of buildings and a definition of very restricted public access zones (access to technical rooms) linked to the activity of collaborators on managerial validation

M6 WEB Staff Digital Identity Management

- All members of M6 Group personnel (permanent staff, casual staff, interns, external service providers, etc.) receive a named user account enabling them to access the M6 Group's data and applications validated by their Manager
- These M6 WEB personnel user accounts are deactivated upon the departure of the collaborator in view of the end of their contract or assignment and permanently deleted after 3 months
- Group M6 requires all its users to protect their user account with passwords consistent with the M6 Group's strategy in terms of length, complexity, expiration and reuse of the password.
- Members of M6 Group personnel are prohibited from sharing identification information or compromising passwords by storing them in or on any unprotected medium in the form of clear and readable text. This obligation is set out in the IT charter.

Privileged accounts

- Privileged accounts or SSH keys (network administrator, system or database account, etc.) are associated with a named identity in order to maximise accountability and verifiability. They are used whenever possible to perform administration tasks only and are not used for reasons of convenience.
- Privileged accounts are not shared unless an application or system does not support multiple dedicated privileged user accounts.
- All user accounts which come preconfigured with new hardware and/or software by default are deactivated. Only named user accounts are used
- Just like user accounts, privileged accounts are deactivated immediately upon the departure of their owner

Networks

- Automatic mechanisms for responding to IT attacks make it possible to block malicious network exchanges by analysing network frameworks (DDOS attack, etc.) or filter requests according to criteria of belonging to lists of global reputation or of other criteria
- Restrictions of resources available on the internet are carried out by filtering at the network level
- Network segregation is achieved at several levels: Between the office automation are and the production areas, between the production areas within ODISO and also between the entities of the M6 Group. Each customer has its own dedicated subnet
- Remote administrator connections are made via VPN only

Servers

- Systems and databases are backed up every evening using an archiving policy. Backups are outsourced to a secure external site
- A real-time monitoring system measuring the availability and consumption of server resources makes it possible to monitor the system and create alerts
- Server security updates are carried out regularly as soon as packages are published
- Restriction of access allows only administrators to connect to servers via named SSH keys

Workstations

- The workstation is equipped with anti-virus software that receives a weekly update of the viral base and performs a hard disk scan twice a week, all of which is supervised by the M6 Group
- An anti-virus mailbox and data feed allow malicious files coming from the internet to be filtered
- Anti-malware and file reputation analysis allow malware and unwanted programs to be blocked before execution
- Windows and major public software (Adobe, VLC, 7zip, etc.) security updates are made during the month of distribution by remote distribution
- Workstations are configured with administration rights restrictions by a central M6 group administration console
- Entering standby mode in the event of inactivity is automatic and requires reopening by entering the password