TECHNICAL AND ORGANIZATIONAL MEASURES

TABLE OF CONTENT

INTRODUCTION

Infobip, in role of a data processor for Services offered to its customers, has implemented and maintains appropriate technical and organizational measures (in further text: measures) in accordance with:

- ISO 27001:2013 and ISO 27002:2013 standards and security control requirements, and
- Article 28, 3 (c) and Article 32 in particular in relation with Article 5, (1) of GDPR.

Measures include physical, ICT and organizational measures to protect processed personal data against unauthorized or unlawful processing and accidental loss, destruction, damage, alteration or disclosure. Measures provide a level of security that is appropriate to the risks of the processing having regard to:

1. the state of the art technology;
2. the costs of implementation;
3. the nature, scope, context and purposes of processing, including the type of personal data; and
4. risk for the rights and freedoms of natural persons that personal data relate to.

DESCRIPTION OF THE TECHNICAL AND ORGANIZATIONAL MEASURES

Infobip has taken significant steps and has invested in implementation and improvement of technical and organizational measures.

To name just a few of the personal data sanitization and protection principles applied and under constant improvement in various Infobip systems:

- Secure data transfer channels between client/supplier systems and Infobip platform (ensuring trustworthy authentication and encryption)
- Implementation of clients' messages' content encryption (while residing on Infobip systems, including CDR archives)
- Centralized identity access management on Infobip messaging platform
- Extensive monitoring & logging systems and centralized management of audit logs
- Ongoing implementation of IDS/IPS/WAF/DDoS solutions for our www and customer portal, as well as internal data centers services
- Ongoing development of parametrized data retention practices (including subsequent methods of data deletion, hashing and/or anonymization, encryption)
- Ongoing harmonization with GDPR requirements of all online and client facing channels, as well as sales/marketing/support processes
- Implementation of industry standard encryption at rest regardless of storage media

Implementation of the measures aims to ensure a level of security which is appropriate to the risk of the specific personal data processing, including:

- Encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- The ability to restore the availability and access to the Customer's Data in a timely manner in the event of a physical or technical incident
- A process for regularly testing, assessing and evaluating the effectiveness of measures for ensuring the security of the processing

Infobip implements these and other measures described in the remainder of this document, taking into account that the measures directly or indirectly contribute to the protection of personal data, but can scope other data under Infobip liability as well.

AUDITS AND ASSESSMENTS

Infobip information systems are subject to extensive audits performed by accredited companies, including ISO 9001 & 27001 and PCI DSS certifications, as well as specialized vulnerability assessment and penetration testing campaigns.

Infobip will use its existing ISO 9001 and 27001 certifications and applicable audit/testing reports to satisfy any external inquiry or audit requests, making these documents available to the Customer or data protection authority on request.

Upon previous agreements and coordination, Infobip agrees to submit its data processing facilities and information resources involved with personal data processing to auditors of 3rd party authorized personnel of the audit (e.g. audit agency personnel) to ascertain compliance with the contracted Services. Prerequisites include receiving audit notice with prearranged timeframe (60 days notice for onsite audit) and entering into a non-disclosure agreement between Infobip and 3rd party performing an audit. Infobip personnel will provide reasonable cooperation in the course of audit, including providing all relevant information and access to all equipment, software, data, files, information systems, etc. used for the performance of Services, including processing of personal data. Unless arranged differently per case, audits shall be carried out at the Customer's or data protection authority's cost and expense.

Audits shall be performed on the basis of the mutually agreed audit plan (limited only to the contracted Services) and shall take due care during their performance not to disturb regular business operations. In case of onsite audit, auditors will not be authorized to export any resources classified as restricted or confidential, i.e. they will be allowed to inspect these only onsite. Infobip reserves the right not to disclose certain information classified as confidential to 3rd parties, even if specifically requested. Maximum effort will be invested in resolution of requests by alternative means. Clients are not allowed to perform more than one on-site check per two (2) years. More frequent audits are allowed only if and to the extend required by Applicable Data Protection Laws (e.g. in case of Personal Data breach).

INFORMATION SECURITY POLICIES

Infobip operates information security management system (ISMS), governed by an information security policy and procedures, approved by the management board. These documented practices are published within the organization and communicated to relevant personnel.
ISMS policies and procedures are subject to regular review and update (if required) to ensure their compliance with the measures.

ORGANIZATION OF INFORMATION SECURITY AND DATA PROTECTION

Information security and personal data protection responsibilities are defined according to the General information security policy, job descriptions and appointment decisions for critical systems. Conflicting duties are identified and separated.
Infobip appointed a data protection officer, possessing appropriate legal competences, who cooperates with members of the Corporate Security department in implementing measures and servers as a contact person for Customer's inquiries related to privacy and personal data protection.
General information security policy defines management's responsibility for information security. All managers deploy information security within their departments as an integral part of core business processes.
Information security is integral part of each project. Projects are organized (planning, quarterly) and implementation tracked regularly; Security measures in projects follow security handbook regulations.
Contacts are maintained with appropriate telecommunication bodies, lawful enforcements entities, privacy agencies etc., by appropriate departments.
Key ICT personnel (administrators) are subscribed to relevant newsletters and maintain their connections with professional organizations, accompanied in large numbers with professional personal certifications.

HUMAN RESOURCE SECURITY

Infobip ensures that employees handle information in accordance with the required level of confidentiality and are aware and behave according to the information resources acceptable use policy. All active employee NDAs define the obligation to keep business secret even after the termination of employment or contractual relationship.

Infobip People Operations department uses legally permissible methods of ensuring that any personnel performing assignments is trustworthy, meets established security criteria and has been, and during the term of the assignment will continue to be, subject to appropriate screening and background verification.

According to applicable Labour laws, all job candidates have to provide applicable evidences of their education.

Infobip ensures that personnel with security responsibilities is adequately trained to carry out security related duties. Infobip has various internal Academy programs for new and existing employees as well as internal newsletter and brochures dealing with information security awareness. All security policies and procedures are available at company's portal with appropriate access rights defined and enforced. Several internal workshops and educations have been conducted on the subject of GDPR.

Specialized security & privacy awareness program is currently under development and will be delivered to all Infobip personnel on regular basis.

Disciplinary process is defined and documented by People Operations department.

ASSET MANAGEMENT

Critical assets associated with information and information processing facilities are identified and an inventory of these assets is maintained in several processing systems.

Acceptable use policy and procedures define rules for acceptable use of assets.

Information is labeled across the processing systems', using natively available labeling options.

Employees leaving the company are obliged, according to the contract, to return all assets in Infobip ownership.

Removable media is not used for personal data processing.

ACCESS CONTROL

Infobip maintains an access control policy, based on business and information security requirements, for facilities, sites, network, system, application and information/data access (including physical, logical and remote access controls).

IT systems are protected by layered defense model, which includes network segmentation, access control lists, usage of firewalls, approval workflow for user/administrator access and other security controls.

User registration and deregistration process is implemented and enforced for all core systems and critical data processing systems. Process flow for user provisioning is defined and enforced on internal systems.

Authentication systems implement personal and unique identifier (user ID) and an appropriate authentication technique, which confirms and ensures the identity of users. Allocation and distribution of authentication information is enforced by the IT systems.

All access privileges are assigned based on the principle of need-to-know and principle of least privilege. Only users with legitimate business reasons use privileged personal accounts for administrative actions requiring higher privileges. Standard personal accounts are used for common tasks.

Access to information systems is controlled by access rights defined per user, group or role depending on type of the system or user concerned.

Passwords are managed according to the defined password baseline. All users are required to change their password at first login where this is possible.

Strong (multi-factor) authentication is used for remote access users, connecting from an untrusted network to production environment (2FA is used for core platform environment).

Privileged use of utility programs is restricted to employees with administrative roles at the systems, while all privilege access activities are logged.

CRYPTOGRAPHY

Cryptographic controls are used to protect personal and sensitive data while stored and transferred.

Clients connecting to Infobip platform via API or Customer User Portal (CUP) have various encryption available for ensuring security of data in transfer and Infobip is encouraging clients to use secure versions of connection methods when connecting to our platform:

- to use international security standards and protocols (SSL encryption) in order to provide secured services – HTTPS, SMPP over SSL
- to use restricted encrypted tunnels that enable secure data transmission between the Customer and Infobip data centre – dedicated IPsec Virtual Private Network (VPN) tunnels
- to use secure file transfer protocol – SFTP

That way customer data (including messages) are secured while in transfer from client's side towards our platform.

Data flows from Infobip towards the message gateways (operators, aggregators) are also protected with secure methods listed above, including other available protocols.

Customer's messages content can be encrypted or masked on client's request:

- Message content encryption – Infobip platform can ensure that all message content is encrypted upon storage in databases. The key for encryption is safely stored and every decryption activity upon client's request requires management approval and is being logged
- Partial content masking – Infobip platform can provide partial content masking in case that client is concerned for the specific parts of messages such as credit card numbers, account numbers etc. Masking is template-based which means that it requires provision of template from client upon which the masking will be based.

Several layers of encryption methods are used on Infobip internal information systems, including: disk/drive, file system and database encryption. End users' workstations connecting to production systems are encrypted.

Infobip implements advanced cryptographic keys protection methods, such as: 3-tier PKI (Public Key Infrastructure), dedicated and isolated keys secure storage and approval workflow for issuing digital certificates (for internal services and externally exposed interfaces).

Usage of secure password and key management solutions, such as KeePass, is encouraged throughout the company.

Infobip continually increases level of protection of personal data by ensuring proper and effective use of cryptography.

PHYSICAL AND ENVIRONMENTAL SECURITY

Infobip ensures protection of information processing facilities against external and environmental threats and hazards, including power/cabling failures and other disruptions caused by failures in supporting utilities. This includes physical perimeter and access protection.

Infobip protects equipment and information received or sent on behalf of the Customer from theft, manipulation and destruction.

All critical production systems are placed within secure datacenters, implementing industry best practices for security & privacy and accredited by numerous leading certificates in the field.

Before use, all ICT equipment is set to comply with company rules. In case of obsoleting or reuse, equipment is either:

- securely wiped of data and obsoleted equipment disposed securely by trusted and certified organizations
- reconfigured using disk images, ensuring secure wipe of all preexisting data

CLOUD SECURITY

Infobip platform is fully cloud-based and designed to ensure that unauthorised persons cannot gain access to data. Access control is performed via NG firewall and centrally administered authentication and authorization mechanism.

Multiple methods for encryption of data in transit from/to the platform are available using leading industry practices (see chapter Cryptography). "Allowed IPs" feature is utilized to limit access per specific user (client) to only a preselected range of public IP addresses, even for unencrypted HTTP access.

Any data removed from our secure system is done so under authorisation of the Data Controller or by authorised personnel for the purpose of data processing.

OPERATIONS SECURITY

Infobip utilizes an established change management system applies to business processes, information processing facilities and systems. Change management system includes tests and approvals during the development/testing/release process, as well as failover (roll back) procedures. Dev/test environment is segregated from production systems and live data are never used for testing purposes.

A specialized “Canary deployment” process is used for ensuring more stable and robust production systems, which is an obligatory control measure for comparing specialized tailored history metrics when releasing new instances of platform services.

Malware protection is used on all servers and endpoints connecting to production systems to ensure secure environment.

Backup copies of production data are created and tested on regular basis to ensure continuous data availability. Redundant hardware and failover capabilities are ensured for backup systems, mostly including offsite (remote) storage. Backups are encrypted, with physically secured access. Hardware failures on media containing production data are handled exclusively by Infobip personnel, i.e. no 3rd party is allowed to transfer the media out of secure data centre premises.

Critical information regarding platform operations and customer data (such as creating, modifying and deleting data, as well as warnings, exceptions, faults and information security events) is properly logged, being monitored and managed 24/7 by Support, Networking and Security Operations teams. Security/audit logs (including successful and failed authentication attempts to core production servers) are collected, analyzed and stored securely on the central logging system. Special (extended) logging principles are applied for PCI DSS scoped environments.

Logging infrastructure upgrade is being implemented in terms of new communication logs management system, offering more robust and scalable solution.

All parts of email system are monitored in detail: antispam servers, main email system servers, load balancers and client access servers.

Alerts are sent from multiple monitoring systems to dedicated mailing groups, supervised by redundant support personnel.

Logs encryption initiative is currently undergoing, aiming to secure maximum possible extent of data, depending on the available technology.

Multiple mature technologies are used for logging and monitoring purposes. Logs retention varies depending on the criticality and storage systems.

Call Data Records (CDRs) containing metadata regarding message traffic are preserved for several months, due to several legitimate business reasons: lawful purposes, tax/audit purposes, billing/dispute processes, clients' requests (troubleshooting, analysis/reports), Detecting, preventing, and investigating spam, fraudulent activity, and network exploits and abuse. PCI DSS and critical security/audit logs are retained for a minimum of 12 months.
Notifiable incidents shall be reported towards authorized bodies and customers according to the data breach management requirements.
Business users are not granted local administrative rights. Software installation to end users' computers is managed centrally or by locally present authorized personnel.
Vulnerabilities of all relevant technologies such as operating systems, databases, applications are managed proactively and in a timely manner, using automated systems where applicable. Vulnerability Assessment scans are performed weekly for our Data Centers public IP address space using tool which provides CVSS Base Score. External penetration tests are conducted at least annually using best practice methodologies: OSSTMM (Open Source Security Testing Methodology Manual), OWASP (Open Web Application Security Project), NIST and ISACA penetration testing; accompanied with audit methodologies, including automated and manual techniques designed to evaluate the security of our target systems. Testing reports are available on demand. Vulnerabilities are managed by dedicated internal security staff who check vulnerabilites and manage patching activities on a daily basis.
Due to these extensive measures, Infobip does NOT allow other 3rd parties (e.g. customers) to perform vulnerability assessment nor penetration testing of our systems.

COMMUNICATIONS SECURITY

Networks are managed solely by dedicated networking department in accordance with policies and related procedures. Access to network equipment (such as routers, firewalls, switches etc.) is restricted to authorized personnel, using individual service accounts and secured channels. No 3rd parties are allowed access on Infobip equipment for configuration or maintenance purposes. Networks are segregated/divided into VLANs and WANs. Several layers of FWs are in operation, protecting publicly available APIs from external attacks and separating DMZ from production systems. Firewall rules are also applied between applications and databases. Access between

these modules are allowed only for specific services that are mandatory for this communication, all other services and ports are blocked using access lists.

Firewall configurations are classified as confidential and therefore NOT available for external disclosure, due to business secrecy and contractual obligations with our clients.

Wireless networks are used only in office spaces (NOT in data centres), segregated and protected with WPA2 security technology.

All network connections and loads are monitored 24/7 by support staff using dedicated applications.

Protection of data in transit is ensured depending on the media:

- Using secure carriers or authorized internal resources for physical media delivery
- Using technical measures enabling confidentiality, integrity and non-repudiation on public networks (see chapter Cryptography)

Business data confidentiality from employees perspective is ensured by security and privacy awareness program and signing of very strict NDA guaranteeing he/she will not misuse confidential information, penalties applied.