link mobility

Data Processing Agreement for LINK's provision of Messaging Services

Security Appendix

Description of the technical and organisational security measures:

IT policies and security practices

1. The Processor maintains and observes IT policies and security practices, which are obligatory for the Processor's employees.
2. The Processor reviews its policies for IT security at least once per year, as well as amends and/or supplements these policies when it deems necessary in order to maintain personal data protection.

Security compliance by the employees

3. The Processor applies a system of organizational measures towards the individuals who process personal data. The Processor's personnel is obliged to:
   - be familiar with the Data Protection Legislation;
   - be familiar with the Processor's privacy policy relevant to the Service and the guidelines for its application;
   - comply with the confidentiality and protection of personal data.
4. The Processor applies measures for personal data protection which guarantee the access to such data only for persons whose professional obligations or a concretely assigned task for implementation of the Service require such access in compliance with the principle "Necessary to know'.

Physical protection concerning access control

5. The Processor maintains appropriate control over the physical access through a system of technical and organizational measures for prevention of unauthorized access to buildings, premises and equipment where the Controller's personal data are processed. This physical security is applied to controlled data centers and controlled zones and premises where the Controller's personal data are stored or processed in another way.
6. The Processor observes the following minimum organizational measures for physical protection:
   - designates zones with controlled access for storage and other forms of processing of personal data;
   - designates zones with controlled access where the elements of the communication-information systems for personal data processing are located;

Договор за обработка на податоци за обезбедување на услуги за пораки од страна на ЛИНК

ДОДАТОК ЗА БЕЗБЕДНОСТ

Опис на техничките и организациските безбедносни мерки:

ИТ политики и безбедносни практики

1. Обработувачот ги одржува и почитува ИТ политиките и безбедносните практики, кои се задолжителни за вработените во Обработувачот.
2. Обработувачот ги прегледува своите политики за ИТ безбедност најмалку еднаш годишно, како и ги менува и/или ги дополнува овие правила кога смета дека е неопходно за да се одржи заштитата на личните податоци.

Усогласеност со безбедноста од страна на вработените

3. Обработувачот применува систем на организациски мерки кон лицата кои обработуваат лични податоци. Персоналот на Обработувачот е должен:
   - да биде запознаен со Законодавството за заштита на податоци ;
   - да биде запознаен за приватноста на обработувачот релевантна за Услугата и упатствата за нејзината примена;
   - да ја почитува доверливоста и заштитата на личните податоци.
4. Обработувачот применува мерки за заштита на личните податоци кои гарантираат пристап до таквите податоци само за лица чии професионални обврски или конкретно зададена задача за спроведување на Услугата бараат таков пристап во согласност со принципот „Потребно е да се знае".

Физичка заштита во врска со контролата на пристапот

5. Обработувачот одржува соодветна контрола врз физичкиот пристап преку систем на технички и организациски мерки за спречување на неовластен пристап до згради, простории и опрема каде што се обработуваат личните податоци на контролорот. Оваа физичка безбедност се применува на контролирани центри за податоци и контролирани зони и простории каде што личните податоци на контролорот се складираат или обработуваат на друг начин.
6. Обработувачот ги почитува следните минимални организациски мерки за физичка заштита:
   - означува зони со контролиран пристап за складирање и други форми на обработка на лични податоци;
   - означува зони со контролиран пристап каде се сместени елементите на комуникацисko-

• maintains systems and policies for organization of the physical access, including to outside persons; • provides technical equipment for physical protection; • provides a team for reaction in the event of personal data breach. 7. The access to the data centers and the controlled zones in the data centers, where Controller's personal data are present, is limited in accordance with the position of the respective employee of the Processor. 8. Any person who enters the data centers or the controlled zones in the data centers, should register upon entrance in the premises, by identifying themselves and should be accompanied by an authorized employee/s of the Processor. Any access authorization should be planned in advance and should require approval by an authorized employee of the Processor. 9. The Processor takes precautionary measures for protection of the physical infrastructure of the data centers from threats, whether there are natural or a result of a human intervention. Document protection 10. The Processor applies appropriate documentary protection as a system of organizational measures during processing of personal data in paper form. 11. The Processor observes the following minimum measures of documentary protection: • establishes and maintains access policy; • regulates the access to the registries; • establishes and maintains procedures for destroying of personal data. IT systems and security of the network 12. The Processor applies protection of the automated information systems and networks through a system of technical and organizational measures for protection from unauthorized access and procession of personal data. 13. The Processor observes the following minimum measures for protection of the automated information systems and networks: • establishes and maintains access policy; • designates roles and responsibilities of the employees having access to systems processing personal data;	информативните системи за обработка на лични податоци ; • одржува системи и политики за организација на физичкиот пристап, вклучително и на надворешни лица; • обезбедува техничка опрема за физичка заштита; • обезбедува тим за реакција во случај на прекршување на личните податоци . 7. Пристапот до центрите за податоци и контролираните зони во центрите за податоци, каде што се присутни личните податоци на контролорот , е ограничен во согласност со позицијата на соодветниот вработен во Обработувачот. 8. Секое лице кое влегува во центрите за податоци или контролираните зони во центрите за податоци, треба да се регистрира при влезот во просториите, со легитимирање и да биде придружуван од овластен/и вработен/и од Обработувачот. Секое овластување за пристап треба да се планира однапред и треба да бара одобрение од овластен вработен во Обработувачот. 9. Обработувачот презема мерки на претпазливост за заштита на физичката инфраструктура на центрите за податоци од закани, без разлика дали се природни или резултат на човечка интервенција. Заштита на документи 10. Обработувачот применува соодветна документарна заштита како систем на организациски мерки при обработката на личните податоци во хартиена форма. 11. Обработувачот ги почитува следните минимални мерки на документарна заштита: • воспоставува и одржува политика за пристап; • го регулира пристапот до регистрите ; • воспоставува и одржува процедури за уништување на лични податоци. ИТ системи и безбедност на мрежата 12. Обработувачот применува заштита на автоматизираните информациски системи и мрежи преку систем на технички и организациски мерки за заштита од неовластен пристап и обработка на лични податоци. 13. Обработувачот ги почитува следните минимални мерки за заштита на автоматизираните информациски системи и мрежи: • воспоставува и одржува политика за пристап; • ги одредува улогите и одговорностите на вработените кои имаат пристап до системите за обработка на лични податоци ; • применува идентификација и автентикација; • применува контроли на сесии;

• applies identification and authentication; • applies session controls; • maintains description of the external connections and of the employees having remote access; • performs supervision of systems, networks and connections in view of eventual attacks or personal data leakage; • provides protection against viruses; • provides copies and back-up copies for restoration (back-up); • describes the information mediums; • prepares and maintains procedures for destruction, deletion or erasure of information mediums. 14. The Processor applies cryptographic protection through a system of technical and organizational measures in view of personal data protection from unauthorized access upon transmission, spreading or provision. 15. The Processor maintains the architecture of documentary security of networks run by it during provision of the Service. The Processor reviews separately this network architecture, including measures for prevention of unauthorized network connections to systems, applications and network devices, in view of compliance with the standards for segmenting, isolating and protection in depth prior to implementation. 16. The Processor maintains measures which are aimed at logical separation, prevention of exposure and unauthorized access to personal data of the Controller. 17. The Processor pseudonymises the personal data of the Controller which is not designated for public and/or unverified access during exchange of personal data of the Controller through public networks by using cryptographic protocol (such as HTTPS, SFTP or FTPS) in view of secure exchange of the data on/via the public networks. 18. The Processor pseudonymises the personal data of the Controller when this is stipulated in the Agreement. If the Service entails management of cryptographic keys, the Processor will maintain the respective procedures for generating, issuance,	• одржува опис на надворешните врски и на вработените со далечински пристап; • врши надзор на системи, мрежи и врски во поглед на евентуални напади или истекување на лични податоци; • обезбедува заштита од вируси; • обезбедува копии и резервни копии за реставрација (резервна копија); • го опишува информативниот медиум; • уништува или брише информациски медиум . 14. Обработувачот применува криптографска заштита преку систем на технички и организациски мерки заради заштита на личните податоци од неовластен пристап при пренос, ширење или обезбедување. 15. Обработувачот ја одржува архитектурата на документарната безбедност на мрежите управувани од него за време на обезбедувањето на Услугата. Обработувачот ја разгледува одделно оваа мрежна архитектура, вклучувајќи мерки за спречување на неовластени мрежни конекции со системи, апликации и мрежни уреди, со оглед на усогласеноста со стандардите за сегментирање, изолирање и длабинска заштита пред имплементацијата. 16. Обработувачот одржува мерки кои се насочени кон логично раздвојување, спречување на изложеност и неовластен пристап до личните податоци на контролорот. 17. Обработувачот ги псевдонимизира личните податоци на контролорот кои не се назначени за јавен и/или непроверен пристап при размена на лични податоци на контролорот преку јавни мрежи со користење криптографски протокол (како што се HTTPS, SFTP или FTPS) со цел безбедна размена на податоците на/преку јавните мрежи. 18. Обработувачот ги псевдонимизира личните податоци на контролорот кога тоа е наведено во Договорот. Доколку Услугата вклучува управување со криптографски клучеви, обработувачот ќе ги одржува соодветните процедури за генерирање, издавање, ширење, складирање, ротација, поништување, обновување, резервна копија, уништување, пристап и користење на таквите клучеви. 19. При обработката на личните податоци на Контролорот, Обработувачот го ограничува пристапот до соодветното најниско ниво потребно за обезбедување и одржување на Услугите. Овој пристап, вклучувајќи го и административниот пристап до сите главни компоненти (привилегиран пристап), е индивидуален, заснован на улога и е предмет на одобрување и редовна валидација од овластен/и вработен/и на Обработувачот, со почитување на

spreading, storage, rotation, annulment, restoration, back-up, destruction, access and use of such keys.	принципите на раздвојување на обврските и минимизирање на обработката.
19. Upon processing of the personal data of the Controller, the Processor limits the access to the respective lowest level necessary for provision and maintenance of the Services. This access, including the administrative access to all main components (privileged access), is individual, based on a role and is subject to approval and regular validation by an authorized employee/s of the Processor, by observing the principles of separation of the obligations and minimization of processing.	20. Обработувачот одржува системи за идентификација и отстранување на непотребни и пасивни сметки со привилегиран пристап и веднаш го отстранува, кога тоа е релевантно, овој пристап по промена на позицијата или престанок на работниот однос, како и на барање на овластени вработени во Обработувачот. , на пример соодветниот директен менаџер.
20. The Processor maintains systems for identification and removal of unnecessary and passive accounts with privileged access and immediately removes, when this is relevant, this access upon change in the position or termination of the employment, as well as at the demand of authorized employees of the Processor, for instance the respective direct manager.	21. Во согласност со стандардните комерцијални практики, обработувачот ги одржува техничките мерки кои бараат затворање на неактивни сесии, блокирање на сметки по неколку последователни неуспешни обиди за влез, силна лозинка или сертификација преку лозинка и мерки кои бараат безбедно пренос и складирање на таквите лозинки.
21. In accordance with the standard commercial practices the Processor maintains the technical measures which demand closure of inactive sessions, blocking of accounts following several consecutive unsuccessful entrance attempts, strong password or certification through a password and measures requiring secure transfer and storage of such passwords.	22. Обработувачот ја контролира употребата на привилегиран пристап и одржува мерки за безбедност на информациите и управување со настани насочени кон: а) идентификување на неовластен пристап и активност; б) олеснување на навремена и соодветна реакција; в) дозволување внатрешни или независни ревизии за усогласеност со важечките политики на Обработувачот.
22. The Processor controls the use of privileged access and maintains measures for security of information and event management aimed at: a) identifying unauthorized access and activity; b) facilitating timely and appropriate reaction; c) allowing internal or independent audits for compliance with the applicable policies of the Processor.	23. Дневниците, во кои се евидентирани привилегираниот пристап и активности, ќе бидат поддржани во согласност со правилата за складирање и одговорност утврдени од Обработувачот. Обработувачот ќе одржува мерки насочени кон заштита од неовластен пристап, модификација и случајно или намерно уништување на таквите дневници.
23. The logs, in which the privileged access and activities are recorded, will be backed up in compliance with the rules for storage and accountability established by the Processor. The Processor will maintain measures aimed at protection from unauthorized access, modification and casual or intentional destruction of such logs.	24. До степен до кој тоа се одржува со функционалноста на соодветниот уред или оперативен систем, обработувачот ја одржува компјутерската безбедност на информациските системи кои содржат лични податоци на контролорот кои вклучуваат, без ограничување на: заклучување на екраните во одредени интервали и решенија за управување на крајни точки кои применуваат конфигурации на безбедноста и барања за крпење, заштитни ѕидови на крајните точки (заштитни ѕидови на крајната точка), шифрирање на целиот простор на дискот, идентификација и отстранување на малициозен софтвер (злонамерен софтвер). Тие се а) редовно ажурирани од централната локација и б) се евидентирани во централната локација точка.
24. To the extent that this is maintained by the functionality of the respective device or operational system, the Processor maintains computer security of the informational systems containing personal data of the Controller which include, without limitation to: locking of screens at certain intervals and solutions for management of endpoints which apply configurations of	Интегритет на активностите и контрола на пристап 25. Обработувачот е должен да :

the security and requirements for patching, protection walls of the endpoints (endpoint firewalls), encrypting of the entire disc space, identification and removal of malicious software (malware). These are a) regularly updated by the central location and b) are logged at the central point. Integrity of the activities and access control 25. The Processor is obliged to: • hold tests for penetration and vulnerability, including automated scanning of the security of the systems and the applications and manual ethical hacking prior to the initial supplies and annually following this; • require from a qualified third party to hold tests for penetration at least once per year; • make automated management and routinely check-ups for compliance of the main components with the requirements of the configuration of the protection; • restore the identified vulnerabilities or incompliance with the requirements for configuration of the security based on the risk associated therewith, exploitation capacity and impact. The Processor takes reasonable steps in order to avoid interruption of the Services when holding its tests, assessments, scans and maintenance activities. • back up systems, containing personal data of the Controller; • guarantee that at least one point of back up is in a location separated from the production systems; • confirm the integrity of the backed-up data through regular holding of tests for restoration of data. 26. The Processor maintains procedures aimed at management of the risks associated with implementation of the changers in its activity. Prior to their integration, the changes in a certain service which is part of the Services, including its systems, networks and main components, will be documented in a request for change, which will include description and a reason for the change, details and schedule for implementation, risk assessment and impact over the service, expected result, plan for reversal and documented approval by an authorized employee/s of the Processor. In the case of discrepancy between the English and Macedonian text, the English text shall prevail.	• прави тестови за пенетрација и ранливост, вклучително и автоматско скенирање на безбедноста на системите и апликациите и рачно етичко хакирање пред првичните набавки и годишно по ова; • бара од квалификувано трето лице да одржува тестови за пенетрација најмалку еднаш годишно ; • направи автоматско управување и рутински контроли за усогласеност на главните компоненти со барањата на конфигурацијата на заштитата; • ги исправи идентификуваните пропусти или неусогласеност со барањата за конфигурација на безбедноста врз основа на ризикот поврзан со тоа, капацитетот за експлоатација и влијанието. Обработувачот презема разумни чекори за да избегне прекин на Услугите при одржувањето на неговите тестови, проценки, скенирања и активности за одржување. • ги архивира системите, кои содржат лични податоци на контролорот; • гарантира дека најмалку една точка за резервна копија е на локација одвоена од производните системи; • го потврди интегритетот на резервните податоци преку редовно одржување на тестови за обновување на податоците. 26. Обработувачот одржува процедури насочени кон управување со ризиците поврзани со имплементацијата на менувачите во неговата активност. Пред нивната интеграција, промените во одредена услуга која е дел од Услугите, вклучувајќи ги нејзините системи, мрежи и главни компоненти, ќе бидат документирани во барање за промена, кое ќе содржи опис и причина за промената, детали и распоред. за имплементација, проценка на ризик и влијание врз услугата, очекуван резултат, план за поништување и документирано одобрување од овластен/и вработен/и на Обработувачот. Во случај на несовпаѓање помеѓу англискиот и македонскиот текст, преовладува англискиот текст.

***