Споразумение за обработване на лични данни по предоставяне на Съобщителни услуги от ЛИНК / Data processing agreement for LINK's provision of messaging services

Сигурност на обработването (*версия на български език)*:

Описание на технически и организационни мерки:

ИТ политики и практики за сигурност

1. ЛИНК поддържа и следва ИТ политики и практики за сигурност, задължителни за служителите на ЛИНК.
2. ЛИНК преразглежда политиките си за ИТ сигурност най-малко веднъж годишно, както и изменя и/или допълва същите, когато сметне за необходимо, за поддържане защитата на личните данни.

Спазване на защитата от служители

3. ЛИНК прилага система от организационни мерки спрямо физическите лица, които обработват лични данни. Персоналът на ЛИНК е длъжен да:
    - познава Приложимото законодателство;
    - познава относимата към Услугата политика за поверителност на ЛИНК и указанията за нейното прилагане;
    - спазва поверителността и защитата на личните данни;
4. ЛИНК прилага мерки за защита на личните данни, гарантиращи достъпа до такива данни само на лица, чиито служебни задължения или конкретно възложена задача за изпълнение на Услугата налагат такъв достъп, при спазване на принципа „Необходимост да знае".

Физическа защита на контрол на достъпа

5. ЛИНК поддържа подходящ контрол върху физическия достъп чрез система от технически и организационни мерки за предотвратяване на неоторизиран достъп до сгради, помещения и съоръжения, в които се обработват лични данни на Администратора. Тази физическа сигурност се прилага за контролирани центрове за данни и контролирани зони и помещения, където се съхраняват или по друг начин обработват личните данни на Администратора.
6. ЛИНК спазва следните минимални организационни мерки на физическа защита:
    - обособява зони с контролиран достъп за съхранение и друга обработка на лични данни;
    - обособява зони с контролиран достъп, в които се разполагат елементите на комуникационно-информационните системи за обработване на лични данни;
    - поддържа системи и политики за организация на физическия достъп, вкл. и на външни лица;
    - осигурява технически средства за физическа защита;
    - осигурява екип за реагиране в случай на нарушение на сигурността на личните данни.
7. Достъпът до центровете за данни и контролираните зони в центровете за данни, в които има лични данни на Администратора, е ограничен според длъжността на съответния служител на ЛИНК.
8. Всяко лице, което влезе в центровете за данни или контролираните зони в центровете за данни, се регистрира при влизане в помещенията, идентифицирайки се, и се придружава от упълномощен/и служител/и на ЛИНК. Всяка оторизация за достъп, се планира предварително и изисква одобрение от упълномощен служител на ЛИНК.
9. ЛИНК взима предпазни мерки, за защита на физическата инфраструктура на центровете за данни от заплахи, както естествени, така и в резултат на човешка намеса.

Защита на документите

10. ЛИНК прилага подходяща документалната защита като система от организационни мерки при - обработването на лични данни на хартиен носител.
11. ЛИНК спазва следните минимални мерки на документалната защита:
    - създава и поддържа политика за достъп;
    - регламентира достъпа до регистрите;
    - създава и поддържа процедури за унищожаване на личните данни.

ИТ системи и сигурност на мрежата

12. ЛИНК прилага защита на автоматизираните информационни системи и мрежи, чрез система от технически и организационни мерки за защита от нерегламентиран достъп и обработка на личните данни.
13. ЛИНК спазва следните минимални мерки за защита на автоматизираните информационни системи и мрежи:
    - създава и поддържа политика за достъп;
    - определя роли и отговорности на служителите с достъп до системи, обработващи лични данни;
    - прилага идентификация и автентикация;
    - прилага контроли на сесията;
    - поддържа описание на външните връзки и на служителите с отдалечен достъп;
    - осъществява наблюдение на системи, мрежи и свързаности за евентуални атаки или изтичане на лични данни;
    - осигурява защита от вируси;
    - осигурява копия и резервни копия за възстановяване (резервираност);
    - описва носителите на информация;

- изготвя и поддържа процедури за унищожаване, заличаване или изтриване на носители.

14. ЛИНК прилага криптографска защита, чрез система от технически и организационни мерки, с цел защита на личните данни от нерегламентиран достъп при предаване, разпространяване или предоставяне.
15. ЛИНК поддържа архитектура на документална сигурността на мрежите, управлявани от него в процеса на предоставяне на Услугата. ЛИНК преглежда отделно тази мрежова архитектура, включително мерки за предотвратяване на неоторизирани мрежови връзки към системи, приложения и мрежови устройства, за спазване на стандартите за сегментиране, изолиране и защита в дълбочина преди изпълнението.
16. ЛИНК поддържа мерки, които са предназначени за логично отделяне, предотвратяване на излагането и неоторизирания достъп до лични данни на Администратора.
17. ЛИНК псевдонимизира личните данни на Администратора, които не са предназначени за публичен и/или непроверен достъп при обмен на личните данни на Администратора през обществени мрежи, като използва криптографски протокол (като HTTPS, SFTP или FTPS) за сигурен обмен на данните по/чрез обществени мрежи.
18. ЛИНК ще псевдонимизира личните данни на Администратора, когато това е предвидено в Договора. Ако Услугата включва управление на криптографски ключове, ЛИНК ще поддържа съответни процедури за генериране, издаване, разпространение, съхранение, ротация, анулиране, възстановяване, архивиране, унищожаване, достъп и използване на такива ключове.
19. При обработка на личните данни на Администратора, ЛИНК ограничава достъпа до съответното най-ниско ниво, необходимо за осигуряване и поддръжка на Услугите. Този достъп, включително административният достъп до всички основни компоненти (привилегирован достъп), е индивидуален, базиран на роля и подлежи на одобрение и редовно валидиране от оторизиран/и служител/и на ЛИНК, следвайки принципите на разделяне на задълженията и минимизация на обработването.
20. ЛИНК поддържа системи за идентифициране и премахване на ненужни и пасивни акаунти с привилегирован достъп и незабавно отменя, когато това е относимо, този достъп при промяна на длъжността или прекратяване на трудовото правоотношение, както и по искане на съответно упълномощени за това служители на ЛИНК, като например съответния пряк ръководител.
21. В съответствие със стандартните търговски практики ЛИНК поддържа техническите мерки, които налагат затваряне на неактивни сесии, блокиране на акаунти след няколко последователни неуспешни опита за вход, силна парола или удостоверяване чрез парола и мерки, изискващи сигурен трансфер и съхранение на такива пароли.
22. ЛИНК контролира използването на привилегирован достъп и поддържа мерки за сигурност на информация и управление на събития, предназначени да: а) идентифицират неразрешен достъп и дейност; б) улесняват своевременното и подходящо реагиране; и в) позволяват вътрешни или независими одити на съответствието с приложимите политики на ЛИНК.
23. Логовете, в които се записват привилегированият достъп и дейности, ще бъдат архивирани в съответствие с установените от ЛИНК правила за съхранение и отчетност. ЛИНК ще поддържа мерки, предназначени да предпазват от неразрешен достъп, модификация и случайно или умишлено унищожаване на такива логове.
24. Доколкото това се поддържа от функционалността на съответното устройство или операционна система, ЛИНК поддържа компютърни защити на информационните системи, съдържащи лични данни на Администратора, които включват без да се ограничават до: заключване на екрани на определено време и решения за управление на крайни точки, които прилагат конфигурации на сигурността и изисквания за пачване (patching), защитни стени на крайните точки (endpoint firewalls), криптиране на цялото дисково пространство, откриване и отстраняване на зловреден софтуер (malware). Същите се: а) актуализират редовно от централната локация и б) логват на централно място.

Интегритет на дейностите и контрол на достъпа

25. ЛИНК е длъжен да:
    - провежда тестове за проникване и уязвимост, включително автоматизирано сканиране на сигурността на системите и приложенията и ръчно етично хакерство преди първоначалните доставки и ежегодно след това;
    - изисква от квалифицирана независима трета страна да провежда тестове за проникване поне веднъж годишно;
    - извършва автоматизирано управление и рутинна проверка на съответствието на основните компоненти с изискванията за конфигурация на защитата;
    - възстановява идентифицираните уязвимости или несъответствие с изискванията за конфигуриране на сигурността въз основа на свързания с тях риск, експлоатационна способност и въздействие. ЛИНК ще предприема разумни стъпки, за да избегне прекъсване на Услугите, когато извършва своите тестове, оценки, сканирания и извършване на дейности по саниране.
    - архивира (back up) системи, съдържащи лични данни на Администратора;
    - гарантира, че поне едно място за архивиране (back up) е на локация, отделена от производствените системи;
    - потвърждава интегритета на архивираните данни чрез регулярно извършване на тестове за възстановяване на данни;

26. ЛИНК поддържа процедури, предназначени да управляват рисковете, свързани с прилагането на промените в дейността му. Преди да бъдат внедрени, промените в дадена услуга, която е част от Услугите, включително нейните системи, мрежи и основни компоненти, ще бъдат документирани в заявка за промяна, която ще включва описание и причина за промяната, подробности и график за изпълнението, оценка на риска и въздействието върху услугата, очакван резултат, план за връщане назад и документирано одобрение от упълномощен/и служител/и на ЛИНК.

Security Appendix (*English version)*:

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;
    - 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;
    - 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, spreading, storage, rotation, annulment, restoration, back-up, destruction, access and use of such keys.
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. 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. 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. 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. 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. 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 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.

***