link mobility

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;
    - 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.

Anexa privind securitatea

Descrierea măsurilor tehnice și organizatorice de securitate:

Politici IT și practici de securitate

1. Procesatorul menține și respectă politicile IT și practicile de securitate, care sunt obligatorii pentru angajații Procesatorului.
2. Procesatorul își revizuiește politicile de securitate IT cel puțin o dată pe an, precum și modifică și/sau completează aceste politici atunci când consideră necesar pentru a menține protecția datelor cu caracter personal.

Respectarea normelor de securitate de către angajați

3. Procesatorul aplică un sistem de măsuri organizaționale față de persoanele care prelucrează date cu caracter personal. Personalul Procesatorului este obligat:
    - să fie familiarizat cu legislația privind protecția datelor;
    - să fie familiarizat cu politica de confidențialitate a Procesatorului relevantă pentru Serviciu și cu liniile directoare pentru aplicarea acesteia;
    - să respecte confidențialitatea și protecția datelor cu caracter personal.
4. Procesatorul aplică măsuri de protecție a datelor cu caracter personal care garantează accesul la astfel de date numai persoanelor ale căror obligații profesionale sau sarcini atribuite în mod concret pentru punerea în aplicare a serviciului necesită un astfel de acces, în conformitate cu principiul "Necesar de cunoscut".

Protecția fizică privind controlul accesului

5. Operatorul menține un control adecvat asupra accesului fizic printr-un sistem de măsuri tehnice și organizaționale pentru prevenirea accesului neautorizat la clădirile, spațiile și echipamentele în care sunt prelucrate datele cu caracter personal ale operatorului. Această securitate fizică este aplicată centrelor de date controlate și zonelor și spațiilor controlate în care datele cu caracter personal ale operatorului sunt stocate sau prelucrate în alt mod.
6. Procesatorul respectă următoarele măsuri organizaționale minime pentru protecția fizică:
    - desemnează zone cu acces controlat pentru stocarea și alte forme de prelucrare a datelor cu caracter personal;
    - desemnează zonele cu acces controlat în care sunt amplasate elementele sistemelor de comunicare-informare pentru prelucrarea datelor cu caracter personal;

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.	• menține sisteme și politici de organizare a accesului fizic, inclusiv al persoanelor din exterior; • furnizează echipamente tehnice pentru protecția fizică; • oferă o echipă de reacție în cazul încălcării securității datelor cu caracter personal. 7. Accesul la centrele de date și la zonele controlate din centrele de date, în care sunt prezente datele cu caracter personal ale operatorului, este limitat în conformitate cu funcția angajatului respectiv al operatorului. 8. Orice persoană care intră în centrele de date sau în zonele controlate din centrele de date trebuie să se înregistreze la intrarea în incintă, identificându-se și trebuie să fie însoțită de unul sau mai mulți angajați autorizați ai Procesatorului. Orice autorizație de acces trebuie planificată în prealabil și trebuie aprobată de un angajat autorizat al Procesatorului. *9.* Procesatorul ia măsuri de precauție pentru protejarea infrastructurii fizice a centrelor de date împotriva amenințărilor, indiferent dacă acestea sunt naturale sau rezultatul unei intervenții umane.
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.	***Protecția documentelor*** 10. Procesatorul aplică o protecție documentară adecvată ca sistem de măsuri organizaționale în timpul prelucrării datelor cu caracter personal pe suport de hârtie. 11. Procesatorul respectă următoarele măsuri minime de protecție a documentelor: • stabilește și menține politica de acces; • reglementează accesul la registre; • stabilește și menține proceduri pentru distrugerea datelor cu caracter personal.
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;	***Sisteme informatice și securitatea rețelei*** 12. Procesatorul aplică protecția sistemelor și rețelelor informatice automatizate printr-un sistem de măsuri tehnice și organizatorice de protecție împotriva accesului și prelucrării neautorizate a datelor cu caracter personal. 13. Procesatorul respectă următoarele măsuri minime de protecție a sistemelor și rețelelor informatice automatizate: • stabilește și menține politica de acces; • desemnează rolurile și responsabilitățile angajaților care au acces la sistemele de prelucrare a datelor cu caracter personal; • aplică identificarea și autentificarea; • aplică controale de sesiune;

- 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

- menține o descriere a conexiunilor externe și a angajaților care au acces la distanță;
- efectuează supravegherea sistemelor, rețelelor și conexiunilor în vederea unor eventuale atacuri sau scurgeri de date personale;
- oferă protecție împotriva virușilor;
- furnizează copii și copii de rezervă pentru restaurare (back-up);
- descrie mediile de informare;
- pregătește și menține procedurile de distrugere, ștergere sau eliminare a mediilor de informații.

14. Procesatorul aplică protecție criptografică printr-un sistem de măsuri tehnice și organizatorice în vederea protecției datelor cu caracter personal împotriva accesului neautorizat la transmitere, răspândire sau furnizare.
15. Procesatorul menține arhitectura de securitate documentară a rețelelor gestionate de acesta în timpul furnizării Serviciului. Procesatorul revizuiește separat această arhitectură de rețea, inclusiv măsurile de prevenire a conexiunilor neautorizate ale rețelei la sisteme, aplicații și dispozitive de rețea, în vederea respectării standardelor de segmentare, izolare și protecție în profunzime înainte de implementare.
16. Procesatorul menține măsuri care vizează separarea logică, prevenirea expunerii și a accesului neautorizat la datele cu caracter personal ale operatorului.
17. Operatorul pseudonimizează datele cu caracter personal ale operatorului care nu sunt destinate accesului public și/sau neverificat în timpul schimbului de date cu caracter personal ale operatorului prin intermediul rețelelor publice prin utilizarea unui protocol criptografic (cum ar fi HTTPS, SFTP sau FTPS) în vederea schimbului securizat de date pe/prin intermediul rețelelor publice.
18. Procesatorul pseudonimizează datele cu caracter personal ale operatorului atunci când acest lucru este stipulat în acord. În cazul în care serviciul implică gestionarea cheilor criptografice, procesatorul va menține procedurile respective pentru generarea, emiterea, răspândirea, stocarea, rotația, anularea, restaurarea, salvarea, distrugerea, accesul și utilizarea acestor chei.
19. La prelucrarea datelor cu caracter personal ale operatorului, procesatorul limitează accesul la nivelul cel mai scăzut respectiv, necesar pentru furnizarea și întreținerea serviciilor. Acest acces, inclusiv accesul administrativ la toate componentele principale (acces privilegiat), este individual,

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	bazat pe un rol și este supus aprobării și validării periodice de către unul sau mai mulți angajați autorizați ai Procesatorului, prin respectarea principiilor de separare a obligațiilor și de minimizare a prelucrării. 20. Procesatorul menține sisteme de identificare și eliminare a conturilor inutile și pasive cu acces privilegiat și elimină imediat, atunci când acest lucru este relevant, acest acces la schimbarea postului sau la încetarea raporturilor de muncă, precum și la cererea angajaților autorizați ai Procesatorului, de exemplu a managerului direct respectiv. 21. În conformitate cu practicile comerciale standard, procesatorul menține măsurile tehnice care impun închiderea sesiunilor inactive, blocarea conturilor după mai multe încercări consecutive de acces nereușite, parola puternică sau certificarea prin parolă și măsurile care impun transferul și stocarea în siguranță a acestor parole. 22. Procesatorul controlează utilizarea accesului privilegiat și menține măsuri de securitate a informațiilor și de gestionare a evenimentelor menite: a) să identifice accesul și activitatea neautorizate; b) să faciliteze reacția promptă și adecvată; c) să permită audituri interne sau independente privind conformitatea cu politicile aplicabile ale procesatorului. 23. Jurnalele, în care sunt înregistrate accesul și activitățile privilegiate, vor face obiectul unei copii de siguranță, în conformitate cu normele de stocare și responsabilitate stabilite de către operator. Procesatorul va menține măsuri de protecție împotriva accesului neautorizat, modificării și distrugerii ocazionale sau intenționate a acestor jurnale. *24.* În măsura în care acest lucru este menținut de funcționalitatea respectivului dispozitiv sau sistem operațional, procesatorul menține securitatea informatică a sistemelor informatice care conțin date cu caracter personal ale operatorului, care includ, fără a se limita la: blocarea ecranelor la anumite intervale și soluții de gestionare a punctelor finale care aplică configurații ale securității și cerințe pentru patch-uri, ziduri de protecție ale punctelor finale (endpoint firewalls), criptarea întregului spațiu de disc, identificarea și eliminarea software-ului malware. Acestea a) sunt actualizate periodic de către punctul central și b) sunt înregistrate la punctul central. ***Integritatea activităților și controlul accesului*** 25. Procesatorul este obligat: • să efectueze teste de penetrare și vulnerabilitate, inclusiv scanarea automată a securității sistemelor și a aplicațiilor și hacking etic manual înainte de livrările inițiale și anual după aceasta;

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 case of discrepancy between the English and Romanian text, the English text shall prevail. ***	• să solicite de la o terță parte calificată să efectueze teste de penetrare cel puțin o dată pe an; • să realizeze o gestionare automată și să verifice în mod regulat conformitatea componentelor principale cu cerințele configurației de protecție; • restabilirea vulnerabilităților identificate sau a nerespectării cerințelor de configurare a securității pe baza riscului asociat acestora, a capacității de exploatare și a impactului. Procesatorul ia măsuri rezonabile pentru a evita întreruperea serviciilor atunci când își desfășoară testele, evaluările, scanările și activitățile de întreținere. • sisteme de back-up, care conțin date cu caracter personal ale operatorului; • garantați că cel puțin un punct de back-up se află într-o locație separată de sistemele de producție; • confirmă integritatea datelor salvate prin efectuarea periodică de teste pentru restaurarea datelor. 26. Procesatorul menține proceduri menite să gestioneze riscurile asociate cu implementarea modificărilor în activitatea sa. Înainte de integrarea lor, modificările într-un anumit serviciu care face parte din Servicii, inclusiv sistemele, rețelele și componentele principale ale acestuia, vor fi documentate într-o cerere de modificare, care va include descrierea și motivul modificării, detaliile și calendarul de implementare, evaluarea riscurilor și a impactului asupra serviciului, rezultatul așteptat, planul de inversare și aprobarea documentată de către un angajat/angajați autorizat(i) al(ai) Procesatorului. În caz de discrepanță între textul în limba engleză și cel românesc, textul în limba engleză va prevala. ***