PROCEDURILE DE MANAGEMENT AL TRAFICULUI

Fiecare domeniu de tehnologie implicat în livrarea unui serviciu către clienții finali are implementată propria politică de gestionare a resurselor disponibile și de prioritizare a unor categorii de trafic în raport cu cerințele specifice impuse de categoria de aplicații care o utilizează. Dimensionarea fiecărui domeniu de tehnologie în parte se face luând în calcul capacitatea maximă necesară susținerii unui profil de trafic normal, evaluat pe baza unui interval de observație de un an pentru eliminarea efectului sezonier, la care se adaugă o margine de capacitate de rezervă, disponibilă pentru utilizare în cazul unor evenimente speciale (creșteri neprevizionate ale traficului peste o anumită valoare într-un interval extrem de scurt de timp, apariția unor defecțiuni ce au condus la rerutarea traficului și la suplimentarea capacității necesare pe un anumit segment).

Orange România asigură suplimentarea resurselor și redimensionarea de capacitate în caz de necesitate astfel încât impactul la nivelul serviciilor oferite clienților finali să nu fie sesizabil. Orange România monitorizează permanent gradul de încărcare al Rețelei, în scopul livrării unei experiențe optime de utilizare a serviciilor oferite către clienții finali. În cadrul procesului de dimensionare a capacității tehnice și a nivelului calitativ oferite de Rețea, Orange România respectă metodologia implementată privitoare la regulile de dimensionare specifice tehnologiilor impactate, standardele existente în industrie precum și analiza rezultatelor obținute de către clienții finali în planurile de îmbunătățire și de evoluție ale arhitecturii Rețelei.

Orange România respectă prevederile Regulamentului 2120/2015 al Parlamentului European și al Consiliului (Regulamentul) referitoare la internetul deschis și acordă clienților săi posibilitatea de a accesa și distribui informații și conținut, de a utiliza și de a pune la dispoziție aplicații și servicii și de a utiliza echipamente terminale la alegere, indiferent de locația utilizatorului final sau a furnizorului, ori de locația, originea ori destinația informațiilor, conținutului sau aplicațiilor oferite prin intermediul Serviciilor de Date și/sau de Internet Fix.

Orange România nu blochează, nu încetinește, nu modifică, nu restricționează, nu interferează cu, nu degradează sau nu discriminează conținut, aplicații sau servicii specifice ori categorii specifice ale acestora decât în situațiile excepționale prevăzute în Regulament și prezentate mai jos, iar în aceste situații excepționale numai dacă este necesar și numai pentru atâta timp cât este necesar:

a) pentru a respecta dreptul Uniunii sau legislația națională conformă cu dreptul Uniunii, sub incidența cărora intră Orange România, sau măsurile conforme cu dreptul Uniunii, menite să pună în aplicare acte legislative ale Uniunii sau legislația națională, inclusiv hotărârile judecătorești sau ale autorităților publice învestite cu competențe în materie;

b) pentru a menține integritatea și securitatea Rețelei Orange România, ale serviciilor furnizate prin intermediul acestei Rețele și ale echipamentelor terminale ale utilizatorilor finali. În cazul atacurilor sau amenințărilor, cum ar fi, dar fără a se limita la atacuri DoS/ DDoS, falsificarea adreselor IP pentru a mima elemente de Rețea sau pentru a permite comunicarea neautorizată, accesul neautorizat la elementele de Rețea sau la echipamentele terminale conectate la Rețea,

Orange Restricted

distribuirea de software malițios sau viruși, Orange România poate aplica măsuri temporare de protecție la nivel de rețea, constând în:

- Filtrarea, limitarea sau chiar blocarea traficului de la sau către adresele IP sau plajele de adrese IP care sunt sursele unui atac sau unei amenințări sau care sunt surse bine cunoscute ale unor astfel de atacuri sau amenințări;
- Blocarea adreselor de IP sau a Servicilor de Date și/sau de Internet fix în cazul unor comportamente suspecte (de ex.: comunicare neautorizată cu elementele Rețelei, falsificare de adrese etc.);
- Blocarea anumitor porturi care constituie o amenințare la securitatea și integritatea Rețelei;

În situația prezentată la litera a) de mai sus, Clientul nu va avea acces la site-urile, aplicațiile, conținutul sau serviciile care fac obiectul actelor legislative menționate.

Aplicarea măsurilor de la litera b) de mai sus va avea loc numai pe durata atacului sau a amenințării. Accesul la conținutul, aplicațiile sau serviciile găzduite de adresele IP care fac obiectul acestor măsuri poate fi blocat. Conținutul, serviciile sau aplicațiile care utilizează porturile care prezintă o amenințare la securitatea sau integritatea Rețelei Orange România pot deveni indisponibile în această perioadă.

În cazul ofertelor care includ un volum specificat de date, după consumarea volumului inclus, Clientul va putea utiliza în continuare Serviciile de Date mobile și/sau de Internet fix, pentru care va fi obligat la plata tarifului specificat în Contract.

În situația în care Clientul se află într-o arie acoperită doar cu tehnologia 2G este posibil ca aplicații de tip video-streaming, interactive speech etc. să nu funcționeze.

În Rețeaua 4G Orange România, conform standardelor ITU, Serviciul de Voce va fi prioritizat față de serviciul de acces la internet pentru a asigura parametrii de calitate necesari pentru funcționarea acestui Serviciu. Lărgimea de bandă necesară pentru traficul VoLTE și semnalizarea aferentă este mică (128 kbps) și nu va afecta Serviciile de Date și/sau de Internet fix.

Orange Restricted