Munca de acasa fara laptop de serviciu – o scurta perspectiva a protecției datelor cu caracter personal

În contextul creat de pandemia de COVD-19, dar nu numai, sunt situații în care angajatorii nu pot pune la dispoziția salariaților echipamente pentru continuarea desfășurarii activitații de acasa, însa le permit acestora sa foloseasca propriile dispozitive - computer, tableta, telefon mobil personal - în scop profesional. Care sunt riscurile pentru angajatori, dar și pentru angajați, în privința protecției datelor cu caracter personal?

Prin intermediul unei politici privind utilizarea propriilor dispozitive (politica de tip BYOD – Bring Your Own Device), angajatorii pot explica angajaților în ce condiții aceștia își pot utiliza echipamentele personale pentru desfășurarea activitații profesionale și ce masuri trebuie sa ia pentru securitatea datelor procesate astfel.

Masurile de siguranța care se impun

Practic, este vorba despre asigurarea protecției pentru doua categorii de date: datele personale ale angajaților care își partajeaza echipamentul pentru efectuarea activitații de serviciu și datele confidențiale ale companiei care sunt acum transferate între rețeaua companiei și echipamentele personale ale angajaților.

Pentru asigurarea protecției datelor (atât a celor care sunt salvate pe echipamentele angajaților, cât și a celor care aparțin companiei, dar sunt accesate la distanța prin intermediul acestor echipamente), este important sa fie implementate anumite masuri de siguranța. Acestea trebuie sa se alinieze la masurile de securitate pe care compania le aplica în cursul normal de desfășurare a activitații și variaza de la implementarea unei soluții antivirus, la obligativitatea parolelor complexe în vederea obținerii accesului la informație, la efectuarea actualizarilor de securitate ale sistemelor de operare, la instalarea de programe tip firewall, la criptarea echipamentelor etc.
În aceste condiții este important sa se stabileasca un echilibru între masurile de securitate solicitate și aplicate de catre companie pe echipamentele angajaților și nevoia acestora din urma de a pastra datele personale într-o zona privata – fara a exista un risc de expunere a acestora.

Cum stabilim echilibrul între personal și profesional?

Având în vedere ca dispozitivele personale conțin, în mod evident, informații privind viața privata a angajaților, trasarea „granitei" între personal și profesional poate fi mai dificila decât în situația utilizarii echipamentelor companiei, iar implementarea masurilor de securitate trebuie sa fie proporționala cu nevoia companiei de a asigura protecția datelor. Cu cât soluțiile avute în vedere pentru asigurarea unor standarde înalte de securitate sunt mai sofisticate (precum monitorizarea activitații angajaților, implementarea unor soluții de tip Data Loss Prevention sau Mobile Device Management), cu atât este mai importanta respectarea cerințelor legale aplicabile în materia protecției datelor.

Astfel, înainte de implementarea unor soluții de acest gen, compania trebuie sa ia în calcul mai multe aspecte. În primul rând, este recomandata limitarea categoriilor de date cu caracter personal ale angajaților prelucrate prin intermediul acestor soluții doar la cele necesare atingerii scopurilor și intereselor legitime de asigurare a securitații datelor. În al doilea rând, este necesara o analiza de evaluare a impactului pe care decizia de a permite angajatului sa lucreze pe dispozitivul personal o va avea asupra protecției datelor. Nu în ultimul rând, este indicata efectuarea în mod corespunzator a testului de balanța pentru interesul legitim (având în vedere ca, în urma analizei fiecarei situații specifice, cel mai probabil interesul legitim va fi temeiul legal în baza caruia pot fi prelucrate datele cu caracter personal ale angajaților stocate prin intermediul propriilor dispozitive).

Nerespectarea obligaţiilor privind asigurarea securităţii datelor cu caracter personal sau privind respectarea drepturilor şi libertăţilor persoanelor vizate (angajaţii în acest caz) poate expune compania la sancţiuni severe, de până la 4% din cifra de afaceri. Mai este de precizat faptul ca o parte semnificativa din sancţiunile aplicate de Autoritatea Naţionala de Supraveghere a Prelucrarii Datelor în ultimele 12 luni (printre care şi cea mai mare sancţiune aplicata până acum în România) au fost impuse ca urmare a unor breşe de securitate. În acest context, devine esenţiala asigurarea unui raport corect între securitatea datelor şi protecţia vieţii private.

Avantajele muncii la distanţa sunt de necontestat în noul context creat de pandemia de COVID-19, însa clarificarea tuturor aspectelor legale care ţin de acest domeniu este esenţiala, având în vedere provocarile cu care se confrunta deja întreg mediul de business.