COVID – 19: Munca de acasa – cum protejam datele cu caracter personal

Munca de acasa a reprezentat pâna de curând o expresie a flexibilității angajatorilor preocupați de asigurarea unui echilibru între viața profesionala și cea personala a angajaților. În contextul pandemiei de Covid-19, munca de pe canapeaua din living sau de la biroul amenajat acasa a devenit o necesitate și ulterior o obișnuința și nu un beneficiu rezervat unui numar relativ mic de angajați. Cum schimbarea s-a petrecut aproape peste noapte, nici angajații, nici angajatorii nu au avut ragazul necesar pentru a se gândi la riscurile la care se expun din perspectiva protecției datelor cu caracter personal. Ce aspecte ar trebui, de fapt, avute în vedere?

Fara îndoiala, munca de acasa impusa de pandemia de Covid-19 a reprezentat o provocare pentru angajatorii chemați sa asigure urgent mijloace eficiente de comunicare pentru un numar semnificativ de angajați. Dar pe lânga punerea la dispoziție a mijloacelor tehnice, aceștia trebuie sa asigure și confidențialitatea datelor și informațiilor pe care angajații le utilizeaza cu ocazia îndeplinirii, de la distanța, a sarcinilor de serviciu, fie ca aceste date și informații aparțin angajatorului, fie ca sunt ale clienților. Iar când este vorba de date cu caracter personal, lucrurile devin și mai stricte, regulile instituite de Regulamentul General privind Protecția Datelor fiind pe deplin aplicabile.

De cealalta parte, deși munca de acasa poate avea avantaje indiscutabile pentru angajați, aceștia trebuie sa fie conștienți ca spațiul de acasa nu a fost conceput pentru a asigura protecția integrala a datelor cu care lucreaza. În plus, departe de birou, apar probleme neașteptate și tentații suplimentare. De exemplu, se poate pierde conexiunea la internet, exact atunci când este nevoie de transmiterea unui document important, iar angajatul se confrunta cu o dilema – se conecteaza la rețeaua nesecurizata a vecinului sau se expune riscului de a nu trimite la timp documentul solicitat.

Pornind de la aceste premise, dar și ca urmare a problemelor care ne-au fost semnalate, am gândit un set de masuri, atât pentru angajatori, cât și pentru angajați, care, odata aplicate, ar putea sa diminueze riscurile asociate muncii de acasa, cel puțin din perspectiva regulilor aplicabile în materia datelor cu caracter personal.

La ce trebuie sa fie atent angajatorul?

1. Așadar, angajatorii ar trebui, în primul rând, sa se asigure ca dispun de resurse IT suficiente, chiar și umane, pe lânga cele tehnice, pentru suportul angajaților. Este mai greu sa faci achiziții de laptopuri, de pilda, în plina criza, dar asigurați-va ca oamenii de la IT controleaza situația.
2. Furnizați, în masura în care este posibil, dispozitive de lucru tuturor angajaților și evitați utilizarea dispozitivelor personale.
3. În situația utilizarii dispozitivelor personale, asigurați-va ca acestea sunt aprobate în prealabil de responsabilii IT.
4. Asigurați-va ca aplicațiile software de securitate instalate pe dispozitivele angajaților sunt actualizate periodic, chiar și de la distanța.
5. Achiziționați sau, daca o aveți deja, utilizați o soluție de tip VPN capabila sa suporte un numar mare de conectari simultane din partea angajaților la rețeaua societații și asigurați-va ca sesiunile la distanța se deconecteaza automat și necesita reautentificare dupa o anumita perioada de inactivitate.
6. Furnizați aplicațiile printr-un canal criptat și puneți la dispoziție canale sigure de comunicare atât între angajați, cât și pentru comunicarea cu exteriorul.
7. Actualizați frecvent sistemul de operare și aplicațiile instalate pe dispozitivele societații.
8. Informați angajații despre riscurile asociate muncii de acasa, precum amenințarile cibernetice și asigurați-va ca toți angajații știu cum sa procedeze în cazul unui potențial incident de securitate.
9. Verificați frecvent activitațile neobișnuite care au loc pe dispozitivele societații și creșteți nivelul de alerta pentru atacuri legate de VPN.

10. Verificați daca în contextul desfășurarii muncii de acasa societatea trebuie sa prelucreze datele angajaților într-un alt mod decât cel obișnuit și asigurați-va ca și în acest caz este respectata legislația în materia protecției datelor.

La ce trebuie sa fie atenți angajații?

1. Utilizați doar reteaua Wi-fi proprie, la care conectarea se face prin intermediul unei parole și nu apelați la rețele publice disponibile atunci când internetul va face probleme. O soluție mult mai sigura, este activarea hotspot-ului pe un alt dispozitiv mobil furnizat de angajator.
2. Nu utilizați dispozitivele personale înainte de a obține aprobarea angajatorului și asigurați-va ca atunci când le folosiți țineți cont de masurile de siguranța și recomandarile aplicabile dispozitivelor de lucru.
3. Conectați-va la rețeaua angajatorului doar prin VPN.
4. Nu printați documente conținând date cu caracter personal sau secrete de afaceri la centre de print sau utilizând imprimanta unei alte persoane și pastrați documentele pe suport hârtie care nu va mai sunt necesare pentru a le distruge la birou într-un mod sigur.
5. Nu raspundeți cererilor de furnizare de date cu caracter personal, în special cele financiare atunci când nu recunoașteți expeditorul și contactați angajatorul pentru a verifica daca acesta are informații cu privire la sursa solicitarii.
6. Nu permiteți persoanelor cu care locuiți sa va acceseze dispozitivele de lucru și asigurați-va ca acestea sunt blocate atunci când nu le utilizați.
7. Asigurați-va ca atunci când sunteți implicat într-o convorbire telefonica sau videoconferința în interes de serviciu, alte persoane nu pot auzi conversația.
8. Evitați utilizarea în interes personal a dispozitivelor de lucru.
9. Anunțați personalul relevant atunci când întâmpinați dificultați în a utiliza anumite resurse IT și nu utilizați aplicații alternative care chiar daca pot face munca mai rapida, nu sunt aprobate de catre angajator (precum emailul personal, website-uri de transfer fișiere).
10. Nu amânați instalarea software-ului antivirus, chiar daca sistemul va da posibilitatea sa faceți acest lucru de câteva ori.
11. Nu publicați pe rețele sociale și nu transmiteți catre alte persoane fotografii cu spațiul de munca cu surprinderea documentelor de lucru sau a monitorului care dezvaluie informații confidențiale sau date cu caracter personal.
12. Anunțați personalul relevant de orice eveniment care ar putea constitui un incident de securitate și respectați procedura aplicabila la nivelul societații în astfel de cazuri.
13. Asigurați-va ca salvați pe cloud-ul angajatorului documentele la care lucrați sau pe baza carora lucrați pentru a asigura disponibilitatea lor în cazul în care nu va mai puteți accesa dispozitivul, de exemplu în cazul unui furt sau în situația în care dispozitivul are probleme tehnice.

Cele mai multe dintre masurile prezentate mai sus ar trebui sa fie incluse deja în procedurile interne privind protecția și securitatea datelor adoptate de orice entitate preocupata de implementarea cerințelor Regulamentului general privind Protecția Datelor.

Cu toate acestea, în contextul pandemiei de Covid-19, este important ca toți angajații sa înțeleaga nevoia sporita de asigurare a protecției datelor cu caracter personal și sa acționeze cu prudența.
Pe de alta parte, angajatorii ar putea sa priveasca situația curenta ca pe un moment propice pentru a verifica eficiența procedurilor interne în fața riscurilor asociate muncii de acasa.