

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 profesională și cea personală 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 obișnuință 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?

Fără îndoială, munca de acasa impusa de pandemia de Covid-19 a reprezentat o provocare pentru angajatorii chemați să asigure urgent mijloace eficiente de comunicare pentru un numar semnificativ de angajați. Dar pe lângă punerea la dispoziție a mijloacelor tehnice, aceștia trebuie să asigure și confidențialitatea datelor și informațiilor pe care angajații le utilizează cu ocazia îndeplinirii, de la distanță, 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 cealaltă parte, deși munca de acasa poate avea avantaje indiscutabile pentru angajați, aceștia trebuie să fie conștienți că spațiul de acasa nu a fost conceput pentru a asigura protecția integrală a datelor cu care lucrează. 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 confruntă cu o dilemă – se conectează la rețeaua nesecurizată 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 măsuri, atât pentru angajatori, cât și pentru angajați, care, odată aplicate, ar putea să diminueze riscurile asociate muncii de acasa, cel puțin din perspectiva regulilor aplicabile în materia datelor cu caracter personal.

La ce trebuie să fie atent angajatorul?

1. Așadar, angajatorii ar trebui, în primul rând, să se asigure că dispun de resurse IT suficiente, chiar și umane, pe lângă cele tehnice, pentru suportul angajaților. Este mai greu să faci achiziții de laptopuri, de pildă, în plină criză, dar asigurați-vă că oamenii de la IT controlează situația.
2. Furnizați, în măsura în care este posibil, dispozitive de lucru tuturor angajaților și evitați utilizarea dispozitivelor personale.
3. În situația utilizării dispozitivelor personale, asigurați-vă că acestea sunt aprobate în prealabil de responsabilii IT.
4. Asigurați-vă că aplicațiile software de securitate instalate pe dispozitivele angajaților sunt actualizate periodic, chiar și de la distanță.
5. Achiziționați sau, dacă o aveți deja, utilizați o soluție de tip VPN capabilă să suporte un număr mare de conectări simultane din partea angajaților la rețeaua societății și asigurați-vă că sesiunile la distanță se deconectează automat și necesită reautentificare după o anumită perioadă 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 societății.
8. Informați angajații despre riscurile asociate muncii de acasa, precum amenințările cibernetice și asigurați-vă că toți angajații știu cum să procedeze în cazul unui potențial incident de securitate.
9. Verificați frecvent activitățile neobișnuite care au loc pe dispozitivele societății și creșteți nivelul de alertă pentru atacuri legate de VPN.

10. Verificați dacă în contextul desfașurării muncii de acasă societatea trebuie să prelucraze datele angajaților într-un alt mod decât cel obișnuit și asigurați-vă că și în acest caz este respectată legislația în materia protecției datelor.

La ce trebuie să fie atenți angajații?

1. Utilizați doar rețeaua 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 sigură, 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-vă că atunci când le folosiți țineți cont de măsurile de siguranță și recomandările aplicabile dispozitivelor de lucru.
3. Conectați-vă 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 păstrați documentele pe suport hârtie care nu va mai sunt necesare pentru a le distruge la birou într-un mod sigur.
5. Nu răspundeți cererilor de furnizare de date cu caracter personal, în special cele financiare atunci când nu recunoașteți expeditorul și contactați angajatorul pentru a verifica dacă acesta are informații cu privire la sursa solicitării.
6. Nu permiteți persoanelor cu care locuiți să vă acceseze dispozitivele de lucru și asigurați-vă că acestea sunt blocate atunci când nu le utilizați.
7. Asigurați-vă că atunci când sunteți implicat într-o convorbire telefonică sau videoconferință 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 dificultăți în a utiliza anumite resurse IT și nu utilizați aplicații alternative care chiar dacă pot face munca mai rapidă, nu sunt aprobate de către angajator (precum emailul personal, website-uri de transfer fișiere).
10. Nu amânați instalarea software-ului antivirus, chiar dacă sistemul vă da posibilitatea să faceți acest lucru de câteva ori.
11. Nu publicați pe rețele sociale și nu transmiteți către alte persoane fotografii cu spațiul de muncă cu surprinderea documentelor de lucru sau a monitorului care dezvăluie 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 aplicabilă la nivelul societății în astfel de cazuri.
13. Asigurați-vă că salvați pe cloud-ul angajatorului documentele la care lucrați sau pe baza cărora 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 măsurile prezentate mai sus ar trebui să fie incluse deja în procedurile interne privind protecția și securitatea datelor adoptate de orice entitate preocupată de implementarea cerințelor Regulamentului general privind Protecția Datelor.

Cu toate acestea, în contextul pandemiei de Covid-19, este important ca toți angajații să înțeleagă nevoia sporită de asigurare a protecției datelor cu caracter personal și să acționeze cu prudență.

Pe de altă parte, angajatorii ar putea să privească situația curentă ca pe un moment propice pentru a verifica eficiența procedurilor interne în fața riscurilor asociate muncii de acasă.