# Udhëzues për përpunimin e të dhënave personale gjatë telepunës në kuadër të masave kundër COVID-19

KOMISIONERI PËR TË DREJTËN
E INFORMIMIT DHE MBROJTJEN
E TË DHËNAVE PERSONALE

**TIRANË, SHKURT 2021**

Zyra e Komisionerit për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale (në vijim *"Zyra e Komisionerit"*), në zbatim të ligjit nr. 9887, datë 10.03.2008 "*Për mbrojtjen e të dhënave personale*", i ndryshuar (në vijim "*Ligji*"), në vijim të publikimit të "*Udhëzuesit për mbrojtjen e të dhënave personale në kuadër të masave kundër COVID-19*", "*Udhëzuesit për përpunimin e të dhënave personale në sektorë specifikë në kuadër ta masave kundër COVID-19*" dhe *"Udhëzuesit për përpunimin e të dhënave personale sipas Protokolleve të Masave Higjieno-Sanitare COVID-19"*, harton këtë Udhëzues, i cili sjell në vëmendje të çdo pale të interesuar disa aspekte konkrete në lidhje me mbrojtjen e të dhënave personale gjatë telepunës, nga situata e krijuar prej pandemisë së shkaktuar nga përhapja e virusit COVID-19.

Gjithashtu, rregullat në këtë udhëzues mbështeten edhe në nenin 15, të Kodit të Punës të Republikës së Shqipërisë, i cili ka parashikuar telepunën si punën që punëmarrësi kryen në shtëpi, ose në një vend tjetër, të përcaktuar në marrëveshje me punëdhënësin, duke përdorur teknologjinë e informacionit dhe komunikimit, brenda kohës së punës sipas kushteve të rëna dakord midis tyre në kontratën e punës.

Respektimi i dinjitetit njerëzor, privatësisë dhe mbrojtjes së të dhënave personale duhet të garantohet në çdo përpunim të të dhënave për qëllime punësimi, për të lejuar zhvillimin e lirë të personalitetit të punonjësit, si dhe për krijimin e mundësive për zhvillimin e marrëdhënieve individuale dhe sociale në vendin e punës.

Për shkak të situatës së shkaktuar nga përhapja e virusit COVID19, punëdhënësit (kontrollues)[1], me qëllim vazhdimin e aktivitetit të tyre, kanë parë si alternativë përdorimin e telepunës si një mënyrë efikase në situata të tilla. Për rrjedhojë, lind nevoja që të orientohen kontrolluesit dhe subjektet e të dhënave në çështjet e garantimit të standardeve të ruajtjes, përpunimit dhe sigurisë së të dhënave personale.

## *1. Kuptimi i Telepunës. Përpunimi i të dhënave personale nga punëdhënësi përmes telepunës.*

Telepuna është një formë e organizimit të punës, e cila nuk zhvillohet në vendin e punës së punëdhënësit, por në ambiente të tjera duke përdorur mjete të teknologjisë së informacionit dhe komunikimit. [2]

Të drejtat e punëdhënësit formalizuar në kontratën e punës dhe legjislacionin specifik, duhet të ushtrohen në respektim të së drejtës së privatësisë dhe të dhënave personale.
Punëdhënësi duhet të justifikojë vënien në zbatim të masave, të cilat duhet të jenë proporcionale me objektivin e synuar. Përpunimi i të dhënave personale nga punëdhënësi duhet të kryhet në përputhje me parimet dhe kriteret e përcaktuara në nenet 5, 6 dhe 7 të Ligjit.

[1] Sipas ligjit nr. 9887, datë 10.03.2008 "*Për Mbrojtjen e të Dhënave Personale*", i ndryshuar, Kontrollues është çdo person fizik ose juridik, autoritet publik, agjenci apo ndonjë organ tjetër që, vetëm apo së bashku me të tjerë, përcakton qëllimet dhe mënyrat e përpunimit të të dhënave personale, në përputhje me ligjet dhe aktet nënligjore të fushës, dhe përgjigjet për përmbushjen e detyrimeve të përcaktuara në këtë ligj.
[2] (neni 15 i Kodit të punës)

Punëdhënësit gjatë monitorimit duhet të respektojnë parimin e mjaftueshmërisë së të dhënave sipas parashikimit të germës *"c"* të pikës 1 të nenit 5 të Ligjit, në të cilën parashikohet se: "*Të dhënat personale mund të mblidhen vetëm nëse është e nevojshme për të arritur një qëllim specifik dhe të mos e tejkalojnë këtë qëllim"*. Për ta vërtetuar këtë, do të duhet të vlerësojnë paraprakisht nëse mbledhja e të dhënave personale të punëmarrësve është proporcionale me qëllimin. Në këtë këndvështrim, nga punëdhënësi duhet të vlerësohet nëse ekziston një mënyrë tjetër më pak ndërhyrëse në jetën private në të cilën të njëjtat rezultate mund të arrihen.

Punëdhënësi, duhet të sigurohet gjithashtu se informon në mënyrë veçanërisht të qartë dhe të plotë për kategoritë e të dhënave personale që mund të mblidhen nëpërmjet mjeteve të teknologjisë së informacionit, sipas nenit 18 të Ligjit.

Informimi duhet të sigurohet në një mënyrë sa më të plotë, në një format të aksesueshëm dhe të përditësuar. Në çdo rast, një informim i tillë duhet të sigurohet përpara se një punëmarrës të kryejë veprimtarinë ose veprimin përkatës dhe të bëhet i disponueshëm menjëherë përmes sistemeve të informacionit që zakonisht përdoren nga punëmarrësi.

Në lidhje me monitorimin e punëmarrësve, çdo punëdhënës (kontrollues) duhet të marrë në konsideratë paraprakisht disa kritere ligjore përpara fillimit të procesit të përpunimit të të dhënave personale. Sipas Ligjit, çdo përpunim i të dhënave personale duhet të ketë një qëllim specifik, të qartë dhe të ligjshëm. Një qëllim i ligjshëm për monitorimin e punonjësve mund të jetë, për shembull, ruajtja e sigurisë së të dhënave personale kur punonjësit punojnë në distancë, sigurimi i respektimit të detyrimeve ligjore ose për të garantuar që një punonjës është duke kryer detyrimet e tij sipas një kontrate pune. Pasi të jetë identifikuar qartë qëllimi i ligjshëm i përpunimit, punëdhënësi duhet të sigurojë që çdo e dhënë personale e mbledhur për këtë qëllim të përpunohet vetëm sa është e nevojshme për atë qëllim specifik, në përputhje me parimin e kufizimit të qëllimit. Çelësi i kësaj procedure do të jetë garantimi që monitorimi i propozuar nga punëdhënësi, të jetë brenda pritshmërive të arsyeshme të punëmarrësve.

Është e rekomandueshme që punëdhënësit të konsultohen me përfaqësuesit e punëmarrësve, në përputhje me legjislacionin specifik ose kontratën kolektive të nënshkruar me sindikatat e këtyre të fundit (në rast se ka), përpara se të aplikohet ndonjë sistem monitorimi duke përfshirë edhe atë me kamera. Ky parim ndiqet edhe në rastet kur parashikohen ndryshime në procesin ose mënyrën e monitorimit të punëmarrësve.

Duke ju referuar parashikimeve të Ligjit, sa i përket mbikëqyrjes së punëmarrësve gjatë procesit të telepunës nuk është e mundur që punëdhënësit të mbështeten vetëm në pëlqimin si bazën ligjore mbi të cilën përpunojnë të dhënat personale të tyre, për shkak të mosbalancimit të pushtetit në marrëdhëniet midis punëdhënësit dhe punëmarrësit, gjë që e bën të vështirë të provohet se pëlqimi është dhënë lirisht. Sipas parashikimit të pikës 24 të nenit 3 të Ligjit "*Pëlqim i subjekteve të të dhënave" është çdo deklaratë me shkrim, e dhënë shprehimisht me vullnet të plotë e të lirë dhe duke qenë në dijeni të plotë për arsyen pse të dhënat do të përpunohen, çka nënkupton që subjekti i të dhënave pranon që të përpunohen të dhënat e tij".*

Kriteret ligjore të përpunimit gjithsesi do të varen nga situata specifike dhe mund të jenë, kur përpunimi i të dhënave personale përmes monitorimit është i domosdoshëm për kryerjen e kontratës së punës, ose është i nevojshëm për respektimin e një detyrimi ligjor të cilit i nënshtrohet punëdhënësi, ose është i nevojshëm për qëllime të interesave legjitime të punëdhënësit (kur kjo nuk rrëzohet nga të drejtat dhe liritë themelore të punëmarrësve). Pra, të zbatohet një nga kriteret e ligjshme të përpunimit të përcaktuara në nenin 6 të Ligjit.

Për të garantuar minimizimin e rreziqeve të mundshme për cenimin e privatësisë nëpërmjet monitorimit të punëmarrësve, duhet të kryhet paraprakisht një vlerësim i ndikimit në mbrojtjen e të dhënave, në rastet kur përpunimi *"ka të ngjarë të rezultojë në një rrezik të lartë për të drejtat dhe liritë e individit"*. Monitorimi i punëmarrësve arrin këtë limit, veçanërisht kur ka monitorim sistematik, kur përdoren teknologji të reja që kanë impakt në privatësi, ose po kryhet një vlerësim bazuar në monitorimin e performancës së tyre.

### *2. Të drejtat e punëmarrësit në cilësinë e subjektit të të dhënave personale.*

Punëmarrësit, në cilësinë e subjekteve të të dhënave personale, mund të ushtrojnë të drejtat që gëzojnë sipas legjislacionit për mbrojtjen e të dhënave personale edhe gjatë telepunës, të tilla si e drejta për akses (neni 12 i Ligjit), e drejta për të kërkuar bllokimin, korrigjimin ose fshirjen (neni 13 i Ligjit), e drejta për të mos qenë subjekt i vendimmarrjes automatike (neni 14 i Ligjit), e drejta për të kundërshtuar (neni 15 i Ligjit) dhe e drejta për t'u ankuar (neni 16 i Ligjit).

Përjashtimet ndaj të drejtave të përmendura më sipër, mund të lejohen nëse parashikohen nga ky Ligj dhe aktet e tjera ligjore specifike që rregullojnë marrëdhënien e punës (kjo në varësi edhe të fushës së punësimit), apo janë një masë e nevojshme në një shoqëri demokratike, për të mbrojtur interesat e sigurinë kombëtare, sigurinë publike, politikën e jashtme, interesat ekonomike dhe financiare të shtetit, parandalimin dhe ndjekjen e veprave penale, mbrojtjen e subjektit të të dhënave ose të drejtat dhe liritë e të tjerëve.

Punëdhënësit duhet të vazhdojnë të mbrojnë të drejtat e punëmarrësve të tyre, duke garantuar që çdo kërkesë e bërë nga këta të fundit të jetë trajtuar në mënyrën e duhur dhe me efikasitet nga personat e ngarkuar, siç mund të jetë edhe Personi i Kontaktit për Mbrojtjen e të Dhënave Personale.

Në lidhje me mbrojtjen e të dhënave personale, punëdhënësit duhet të ofrojnë trajnime specifike për punëmarrësit e tyre. Gjithashtu, kanë detyrimin e përditësimit të udhëzuesve/rregulloreve të tyre të brendshme, në aspektin e aksesit dhe përpunimit të të dhënave personale në kuadër të marrëdhënies së punës në kushtet e reja të organizimit të punës.

Punëdhënësit duhet të angazhohen në kuadër të informimit të punëmarrësve mbi përdorimin e mekanizmave të përpunimit të të dhënave në kuadër të telepunës (si p.sh., video-konferencat, etj.) dhe masat në kuadër të garantimit të sigurisë së të dhënave personale.

Gjithashtu, punëdhënësit duhet në çdo rast të informojnë punëmarrësit për mënyrat e reja të monitorimit dhe përpunimit të të dhënave personale, si dhe të japin udhëzime praktike për përdorimin e pajisjeve elektronike në mënyrën e duhur dhe të sigurtë. Punëdhënësit mund të udhëzojnë punëmarrësit për mënyrën si dhe kur do të lejohet regjistrimi i video-konferencave, duke specifikuar kufizimin e regjistrimeve sistematike të tyre dhe ndarjen (sharing) e të tilla regjistrimeve me persona të tretë të paautorizuar. Punëdhënësit duhet të ofrojnë informacione të kuptueshme dhe të sakta për punëmarrësit në lidhje me mekanizmat (settings) që të tilla pajisje ofrojnë, për të garantuar sigurinë e të dhënave.

### *3. Masat për sigurinë e të dhënave*

Situata e krijuar nga COVID-19, solli si nevojë përdorimin gjerësisht të telepunës. Kjo situatë mund të çojë potencialisht në devijim të mundshëm nga proceset standarde të punës dhe vështirësi për të siguruar mjete të automatizuara gjatë telepunës, kështu që ekziston një mundësi më e lartë e shkeljeve të të dhënave personale për shkak të gabimit njerëzor.

Aplikimi për herë të parë ose rritja e përdorimit të mjeteve të telepunës mund të ngrejë si problem çështjen e marrjes së masave shtesë lidhur me sigurinë e të dhënave.

Në këtë kuadër, punëdhënësit duhet të hartojnë rregulla lidhur me sigurinë e të dhënave në kuadrin e telepunës, që duhen respektuar, në përputhje me parashikimet e neneve 27 dhe 28 të Ligjit, si dhe të hartojnë një dokument informues në kuadër të telepunës, me qëllim vendosjen në dispozicion të punëmarrësve në mënyrë që të njihen dhe ta zbatojnë në praktikë.

Në kuadër të këtyre masave, punëdhënësi duhet të vendosë në dispozicion të punëmarrësve një listë pajisjesh/mjetesh komunikimi apo të punës në grup, që të jenë të përshtatshme për punën në distancë. Ato duhet të garantojnë konfidencialitetin e të dhënave personale dhe informacioneve që transmetohen dhe aksesohen nga punonjësit, p.sh., përdorimi i një VPN[3] për të shmangur ekspozimin e drejtpërdrejtë të shërbimeve në internet.

Disa masa praktike që mund të merren për t'i mbajtur të dhënat personale të sigurta dhe konfidenciale gjatë punës jashtë zyrës janë:

**Në lidhje me pajisjet:**

- Të garantohet që çdo pajisje të ketë përditësimet e nevojshme, si përditësimet e sistemeve operative (si IOS ose Android) dhe përditësimet e software-it dhe antiviruset;
- Të sigurohet kompjuteri, laptopi ose pajisja në një vendndodhje të sigurt;
- Të tregohet kujdes që pajisje të tilla si USB, telefona, laptopë ose tabletë të mos humbasin;
- Të bllokohet pajisja nëse duhet ta lini atë pa mbikëqyrje për çfarëdolloj arsyeje;

[3] Një VPN, ose Rrjet Virtual Privat, ju lejon të krijoni një lidhje të sigurt me një rrjet tjetër përmes internetit. VPN-të mund të përdoren për të hyrë në faqet e internetit të kufizuara në rajon, për të mbrojtur aktivitetin tuaj të shfletimit nga sytë kureshtarë në Wi-Fi publike etj.

- Të sigurohet që pajisjet të jenë të fikura, të kyçura ose të ruajtura me kujdes kur nuk përdoren;
- Të përdoren kontrolle efektive të aksesit në pajisje (të tilla si vërtetimi me shumë faktorë dhe fjalëkalime të forta) dhe, kur është e nevojshme, enkriptim për të kufizuar hyrjen në pajisje dhe për të zvogëluar rrezikun nëse një pajisje është vjedhur ose zhvendosur;
- Kur një pajisje humbet duhet të ndërmerren menjëherë hapa për të siguruar fshirjen e kujtesës në distancë, aty ku është e mundur.

**Në lidhje me Email-et:**

- Të ndiqen të njëjtat politika që zbatohen në institucion ose shoqëri, rreth përdorimit të postës elektronike;
- Të përdoren llogari të postës elektronike të punës, në vend të asaj personale. Nëse duhet të përdoret e-mail personal sigurohuni që përmbajtja dhe informacionet ose dokumentet bashkëngjitur të jenë të koduara;
- Para se të dërgohet një e-mail, të sigurohet që po iu dërgohen marrësve të saktë, veçanërisht për postat elektronike që përfshijnë sasi të mëdha të të dhënave personale ose të dhëna sensitive.

**Në lidhje me *Cloud*[4] dhe hyrjen në rrjet:**

- Kur është e mundur, të përdoren vetëm rrjetet e besuara të institucionit ose shërbimet *Cloud*, dhe në përputhje me rregullat dhe procedurat organizative në lidhje me *cloud* ose hyrjen në rrjet, aksesin dhe përhapjen/transmetimin e të dhënave;
- Nëse nuk është duke u punuar në *cloud* ose pa hyrje në rrjet, sigurohuni që çdo e dhënë e përpunuar është e ruajtur në mënyrë të përshtatshme dhe të sigurt.

Këto masa duhen marrë në kuadër të zbatimit të Udhëzimit nr. 47, datë 14.09.2018, *"Për përcaktimin e rregullave për ruajtjen e sigurisë së të dhënave personale të përpunuara nga subjektet përpunuese të mëdha"* dhe Udhëzimit nr. 48, datë 14.09.2018, *"Për certifikimin e sistemeve të menaxhimit të sigurisë së informacionit, të dhënave personale dhe mbrojtjes së tyre"*, të miratuara nga Zyra e Komisionerit.

### *4. Integriteti dhe konfidencialiteti*

Punëmarrësit, gjatë telepunës, përdorin shpesh pajisjet e tyre personale (kompjuter, laptop, telefon smart) për qëllime profesionale dhe mbështeten në lidhjet VPN për të aksesuar në distancë sistemet informatike të kompanive, të cilat mund të çojnë në rritje të nivelit të riskut për punëdhënësit.

Punëdhënësi duhet të zbatojë masa të përshtatshme sigurie dhe mund të jetë e nevojshme të përditësojë politikat e sigurisë dhe dokumentacione të tjera të brendshme, për të adresuar çështje

[4] *Praktika e përdorimit të një rrjeti serverësh në internet për të ruajtur, menaxhuar dhe përpunuar të dhëna, në vend të një serveri lokal ose një kompjuteri personal.*

specifike të tilla si puna nga shtëpia dhe BYOD[5]. BYOD-i në vetvete nuk është "përpunim të dhënash personale", por një mjet teknik i veçantë mbi të cilin mbështeten përpunimet.

Përdorimi i pajisjeve personale varet nga zgjedhja e punëdhënësit, i cili mundet njëkohësisht ta autorizojë këtë me disa kushte, ose ta ndalojë krejtësisht.

Punëdhënësit duhet të informojnë punëmarrësit për ekzistencën e këtyre rreziqeve (si p.sh. hacker-at kompjuterikë që dërgojnë e-maile peshkuese, të njohura si phishing[6] emails ose spame), pasi humbja, shkatërrimi ose aksesi i paautorizuar në të dhënat personale, pavarësisht nëse është aksidental apo i paqëllimtë, konsiderohet shkelje e të dhënave personale sipas Ligjit.

**Si t'i reduktojmë këto rreziqe?**

Në vijim disa masa praktike që mund të aplikohen në këtë rast:

- Të izolohen pjesët e pajisjes personale që ka të ngjarë të përdoren në një kuadër profesional;
- Të kontrollohet aksesi nga distanca nëpërmjet një tërësie masash të autentifikimit të përdoruesit (nëse është e mundur, me anë të një certifikate elektronike, karte SIM, etj.);
- Të aplikohen masa të kodimit të qarkullimeve të informacioneve (VPN, HTTPS[7], etj.);
- Të kërkohet respektimi i masave elementare të sigurisë sikurse kyçja e pajisjes me një fjalëkalim në përputhje me praktikat e mira dhe përdorim të një antivirusi të përditësuar;
- Të ndërgjegjësohen përdoruesit në lidhje me rreziqet e mundshme, të ndahen zyrtarisht përgjegjësitë për secilin dhe të saktësohen masat parandaluese që duhen zbatuar në një dokument me forcë detyruese.

### *5. Përpunimi i të dhënave të personale dhe monitorimi i punonjësve përmes kamerave*

Konstatohet një tendencë e punëdhënësve publikë dhe privatë (në cilësinë e kontrolluesit) për të monitoruar punëmarrësit në kuadër të marrëdhënies së punës, duke përdorur mekanizma, mënyra dhe mjete të ndryshme. Një mënyrë mjaft e përhapur monitorimi është edhe ajo përmes kamerave.

Parimi i mjaftueshmërisë së të dhënave personale, parashikuar në germën *"c"*, të pikës 1 të nenit 5 të Ligjit, nënkupton faktin që kontrolluesit (publikë ose privatë) duhet të mbledhin dhe përpunojnë të dhënat personale në përputhje me qëllimin e përpunimit dhe të mos e tejkalojnë këtë qëllim.

---

[5] *Përdorimi i pajisjeve informatike personale në një kontekst profesional njihen me akronimin "BYOD", i cili është shkurtimi i shprehjes angleze "Bring Your Own Device"*

[6] *Praktika mashtruese e dërgimit të postës elektronike që pretendon të jetë nga kompani me reputacion në mënyrë që të nxisë individët të zbulojnë informacione personale, të tilla si fjalëkalimet dhe numrat e kartave të kreditit, etj.*

[7] *Hypertext Transfer Protocol Secure (HTTPS) - Versioni i sigurt i HTTP, i cili është protokolli kryesor që përdoret për të dërguar të dhëna midis një shfletuesi dhe një faqe në internet. HTTPS është e koduar në mënyrë që të rrisë sigurinë e transferimit të të dhënave. Kjo është veçanërisht e rëndësishme kur përdoruesit transmetojnë të dhëna të ndjeshme, të tilla si hyrja në një llogari bankare, shërbimi i postës elektronike ose ofruesi i sigurimit shëndetësor.*

Në mënyrë të ngjashme, punëdhënësi duhet të vlerësojë nëse është proporcionale mbledhja e të dhënave në lidhje me kohën dhe frekuencën e pushimeve të punonjësve për të monitoruar punën e tyre nga shtëpia, cilat të dhëna janë të nevojshme për të garantuar sigurinë e sistemeve informatike të punëdhënësit (p.sh., aktivizimi i kamerës së pajisjes, regjistrimi i lëvizjeve të mouse-it, fotografime të ekranit), etj.

Monitorimi i punëmarrësit me qëllim mbikëqyrjen e punës, nëpërmjet sistemit të video-survejimit (CCTV), është parimisht i ndaluar. Kamerat nuk mund të përdoren për mbikëqyrjen e një punonjësi në vendin e punës. Vendosja e kamerave në ambientet e punës së punonjësve, zyrë apo shtëpi me qëllim mbikëqyrjen apo vlerësimin e performancës është parimisht në kundërshtim me parashikimet e ligjit dhe akteve nënligjore, konkretisht Udhëzimit nr. 11, datë 08.09.2011, të Komisionerit mbi *"Përpunimin e të dhënave personale të punonjësve në sektorin privat"*, i ndryshuar.

Ndërkohë, përdorimi i CCTV (kamera e pajisjes së punës) me qëllim komunikimin me punëdhënësin gjatë telepunës është në vlerësimin e këtij të fundit. Është në kompetencë të punëdhënësit (kontrolluesi) të përcaktojë qëllimin dhe mënyrat e përpunimit të të dhënave, në funksion të veprimtarisë së tij, duke respektuar parashikimet e legjislacionit për mbrojtjen e të dhënave personale.

Disa platforma video-konference lejojnë administruesit e eventeve, të analizojnë vëmendjen e pjesëmarrësve të tyre në kohë reale ndërsa disa të tjera, lejojnë regjistrimin e takimeve. Të tilla regjistrime mund të përfshijnë zërin e pjesëmarrësve, komunikimet me mesazhe, fytyrat, ambientin privat në shtëpi (që kapen nëpërmjet kamerës së webit) sikurse edhe ekranin që ndahet nga folësit. Disa faqe interneti të tjera mundësojnë transkriptime automatike.

Në parim, punëdhënësit nuk duhet të detyrojnë aktivizimin e kamerës për punëmarrësit që marrin pjesë në video-konferencë.

Telepuna mund të cenojë të drejtën për respektim të privatësisë, sidomos të personave të tjerë të pranishëm në banesë. Për këtë shkak, një punëmarrës në parim mund të refuzoj transmetimin e imazheve të tij gjatë një video-konference, duke theksuar arsyet që lidhen me situatën e tij të veçantë. Vetëm në rrethana tepër të veçanta, të cilat i takon punëdhënësit t'i përcaktojë dhe justifikojë, mund të bëhet e nevojshme pjesëmarrja me fytyrë në video-konferencë.

Gjithashtu, punëdhënësi nuk mund të përdorë një pajisje të mbikëqyrjes së përhershme. Nëse punëdhënësit i lind e drejta të kontrollojë aktivitetin e punëmarrësve të tij, ai nuk mund t'i vendosë ata nën mbikëqyrje të përhershme, përveçse në raste përjashtimore, të cilat duhet të jenë të justifikuara në mënyrën e duhur në raport me natyrën e detyrës së ngarkuar.

### *6. Regjistrat fizikë / dokumentet shkresore*

Është e rëndësishme të theksohet se mbrojtja e të dhënave personale, gjatë telepunës, zbatohet jo vetëm për të dhënat personale që përpunohen në mënyrë elektronike, por edhe për të dhënat personale që përpunohen në mënyrë manuale (hard copy).

Gjatë telepunës, përdorimi i shkresave apo dokumenteve duhet të shoqërohet me ndërmarrjen e masave specifike nga ana e punëdhënësit për të garantuar sigurinë dhe konfidencialitetin e tyre. Dokumentet specifike që mund të nxirren nga ambientet jashtë pune, duhet të mbahen duke u siguruar që ato të mos humbasin ose të aksesohen nga persona të paautorizuar. Kur është e mundur, punëdhënësi duhet të mbajë evidenca në formë të shkruar se cilat dokumente janë marrë në shtëpi.

***

*Ky Udhëzues përmban orientime të përgjithshme (jo shteruese) në lidhje me përpunimin e të dhënave personale gjatë telepunës si dhe masat e sigurisë që duhet të ndërmarrë çdo kontrollues (punëdhënës) në kuadër të garantimit të përpunimit të ligjshëm të të dhënave personale.*

*Duhet theksuar se, detyrimet që lindin ndaj çdo kontrolluesi gjatë telepunës dallojnë në bazë të specifikave të veprimtarisë së punës dhe procesit të përpunimit të të dhënave personale dhe aplikohen rast pas rasti.*

*Dispozitat e këtij Udhëzuesi janë të zbatueshme për aq sa është e mundur edhe për procesin e zhvillimit të veprimtarisë mësimore në ciklin e mesëm shkollor dhe në arsimin e lartë universitar, nga të gjitha strukturat publike dhe private që përdorin platformat "online" të mësimdhënies të tilla si Microsoft Teams, Zoom, Webex, Google Classroom, etj.*