F NEX — TRUST CENTER

Politika e Privatësisë dhe Mbrojtjes së të Dhënave

Versioni në gjuhën shqipe

Hyrje

Si pjesë e përgjegjësisë së saj korporative, F NEX është e përkushtuar ndaj zbatimit të ligjeve kombëtare dhe ndërkombëtare për mbrojtjen e të dhënave. Kjo Politikë e Mbrojtjes dhe Privatësisë së të Dhënave bazohet në parime të shëndosha dhe të pranuara globalisht për mbrojtjen e të dhënave. Sigurimi i mbrojtjes së të dhënave është themeli i krijimit dhe ruajtjes së marrëdhënieve të besueshme biznesi, mbrojtjes së interesave të klientëve, si dhe reputacionit të F NEX.

Politika e Privatësisë dhe Mbrojtjes së të Dhënave ofron një nga kushtet e nevojshme kornizë për transmetimin ndërkufitar të të dhënave të kryer nga F NEX. Ajo siguron nivelin e duhur të mbrojtjes së të dhënave të përcaktuar nga Direktiva e Bashkimit Evropian për Mbrojtjen e të Dhënave, Rregullorja e Përgjithshme e Mbrojtjes së të Dhënave (GDPR), si dhe ligjet kombëtare për transmetimin ndërkufitar të të dhënave, duke përfshirë vendet që ende nuk kanë ligje të përshtatshme për mbrojtjen e të dhënave.

Kjo Politikë e Privatësisë dhe Mbrojtjes së të Dhënave vlen për F NEX Shpk, të regjistruar në Shqipëri, duke përfshirë të gjithë punonjësit e saj. Politika e Mbrojtjes së të Dhënave shtrihet në të gjitha përpunimet e të Dhënave Personale. Kjo politikë e Mbrojtjes së të Dhënave përfshin parimet e privatësisë së të dhënave të pranuara ndërkombëtarisht, përfshirë GDPR-në, pa zëvendësuar ligjet ekzistuese kombëtare. Ajo plotëson ligjet kombëtare të privatësisë së të dhënave.

Përkufizime dhe Parime për Përpunimin e të Dhënave Personale

Përkufizime

- **Të dhënat anonimizohen** nëse identiteti personal nuk mund të gjurmohet kurrë nga askush, ose nëse identiteti personal mund të rikrijohet vetëm me një sasi të paarsyeshme kohe, shpenzimesh dhe pune.
- **Pëlqimi** është marrëveshja vullnetare dhe ligjërisht e detyrueshme për përpunimin e të dhënave.
- **Incidentet e Mbrojtjes së të Dhënave** janë të gjitha ngjarjet ku ekziston dyshim i justifikuar se të dhënat personale po aksesohen, mblidhen, modifikohen, kopjohen, transmetohen ose përdoren në mënyrë të paligjshme. Kjo mund të lidhet me veprime nga palë të treta ose punonjës.
- **Subjekti i të dhënave** sipas kësaj Politike për Mbrojtjen e të Dhënave është çdo person fizik, të dhënat e të cilit mund të përpunohen. Në disa vende, subjekte të të dhënave mund të jenë edhe personat juridikë.
- **Të dhënat shumë të ndjeshme** janë të dhëna në lidhje me origjinën racore dhe etnike, mendimet politike, besimet fetare ose filozofike, anëtarësimin në sindikata ose shëndetin dhe jetën seksuale të

subjektit të të dhënave. Sipas ligjit kombëtar, kategoritë e mëtejshme të të dhënave mund të konsiderohen shumë të ndjeshme ose përmbajtja e kategorive të të dhënave mund të strukturohet ndryshe. Për më tepër, të dhënat që lidhen me një krim shpesh mund të përpunohen vetëm sipas kërkesave të veçanta.

- **Të dhënat personale** janë të gjitha informacionet në lidhje me persona fizikë të caktuar ose të përcaktueshëm. Një person përkufizohet për shembull nëse marrëdhënia personale mund të përcaktohet duke përdorur një kombinim informacioni me njohuri shtesë edhe të rastësishme.
- **Përpunimi i të dhënave personale** do të thotë çdo proces, me ose pa përdorimin e sistemeve të automatizuara, për të mbledhur, ruajtur, organizuar, mbajtur, modifikuar, kërkuar, përdorur, përcjellë, transmetuar, shpërndarë ose kombinuar dhe krahasuar të dhëna. Kjo përfshin gjithashtu asgjësimin, fshirjen dhe bllokimin e të dhënave dhe të mediave të ruajtjes së të dhënave.
- **Përpunimi i të dhënave personale është i detyrueshëm** nëse qëllimi i lejuar ose interesi i justifikuar nuk mund të arrihet pa të dhënat personale, ose vetëm me shpenzime jashtëzakonisht të larta.
- **Kontrolluesi i të Dhënave** është kompania ligjërisht e pavarur, aktiviteti i biznesit të së cilës përcakton masën përkatëse të përpunimit.
- **Palët e treta** janë kushdo përveç subjektit të të dhënave dhe Kontrolluesit të të Dhënave.
- **Transmetimi** është çdo zbulim i të dhënave të mbrojtura nga subjekti përgjegjës ndaj palëve të treta.
- **Vendet e treta** sipas politikës së Mbrojtjes së të Dhënave janë të gjitha kombet jashtë Bashkimit Evropian/EEA-së. Kjo nuk përfshin vendet me një nivel mbrojtjeje të të dhënave që konsiderohet i mjaftueshëm nga komisioni i BE-së.

Parimet për Përpunimin e të Dhënave Personale

1. Drejtësi dhe Ligjshmëri

Gjatë përpunimit të të dhënave personale, të drejtat individuale të subjekteve të të dhënave duhet të mbrohen. Të dhënat personale duhet të mblidhen dhe përpunohen në mënyrë të ligjshme dhe të drejtë.

2. Kufizimi në një Qëllim Specifik

Të dhënat personale duhet të përpunohen vetëm për qëllimin që është përcaktuar para mbledhjes së të dhënave. Ndryshimet e mëvonshme të qëllimit janë të mundshme vetëm në një masë të kufizuar dhe kërkojnë justifikim.

3. Transparenca

Subjekti i të dhënave duhet të informohet se si po trajtohen të dhënat e tij/saj. Në përgjithësi, të dhënat personale duhet të mblidhen direkt nga individi në fjalë. Kur mblidhen të dhënat, subjekti i të dhënave duhet të jetë në dijeni ose të informohet për:

- Identiteti i Kontrolluesit të të Dhënave.
- Qëllimi i përpunimit të të dhënave.
- Palët e treta ose kategoritë e palëve të treta të cilave mund t'u transmetohen të dhënat.

4. Reduktimi i të Dhënave dhe Ekonomia e të Dhënave

Para përpunimit të të dhënave personale, duhet të përcaktohet nëse dhe në çfarë mase përpunimi i të dhënave personale është i nevojshëm për të arritur qëllimin për të cilin ndërmerret. Kur qëllimi e lejon dhe kur shpenzimet e përfshira janë në përpjesëtim me qëllimin që ndiqet, duhet të përdoren të dhëna anonime ose statistikore. Të dhënat personale nuk mund të mblidhen paraprakisht dhe të ruhen për qëllime të mundshme në të ardhmen, përveç nëse kërkohet ose lejohet nga ligji kombëtar dhe GDPR.

5. Fshirja

Të dhënat personale që nuk nevojiten më pas skadimit të periudhave ligjore ose të lidhura me procesin e biznesit duhet të fshihen. Mund të ketë një tregues të interesave që meritojnë mbrojtje ose rëndësisë historike të këtyre të dhënave në raste individuale. Nëse po, të dhënat duhet të mbeten në dosje derisa interesat që meritojnë mbrojtje të jenë sqaruar ligjërisht, ose arkivi i korporatës të ketë vlerësuar nëse ato duhet të ruhen për qëllime historike.

6. Saktësia Faktike dhe të Dhënat e Përditësuara

Të dhënat personale në dosje duhet të jenë të sakta, të plota dhe - nëse është e nevojshme - të mbahen të azhurnuara. Duhet të ndërmerren hapa të përshtatshëm për të siguruar që të dhënat e pasakta ose të paplota të fshihen, korrigjohen, plotësohen ose azhurnohen. Subjekti i të dhënave ka të drejtë të hyjë dhe të azhurnojë të dhënat e tij përmes një kërkese drejtuar zyrtarit të Mbrojtjes së të Dhënave.

7. Konfidencialiteti dhe Siguria e të Dhënave

Të dhënat personale i nënshtrohen sekretit të të dhënave. Ato duhet të trajtohen si konfidenciale në nivel personal dhe të mbrohen me masa të përshtatshme organizative dhe teknike për të parandaluar aksesin e paautorizuar, përpunimin ose shpërndarjen e paligjshme, si dhe humbjen, modifikimin ose shkatërrimin aksidental.

Besueshmëria e Përpunimit të të Dhënave

Mbledhja, përpunimi dhe përdorimi i të dhënave personale lejohet vetëm sipas bazave ligjore të mëposhtme. Një nga këto baza ligjore kërkohet gjithashtu nëse qëllimi i mbledhjes, përpunimit dhe përdorimit të të dhënave personale duhet të ndryshohet nga qëllimi fillestar.

Të Dhënat e Klientëve dhe Partnerëve

C.1. Përpunimi i të Dhënave Gjatë Aktiviteteve të Shitjes me Klientët Potencialë

Të dhënat personale të klientëve potencialë, partnerëve dhe partnerëve përkatës mund të përpunohen me qëllim krijimin, ekzekutimin dhe përfundimin e një kontrate. Kjo gjithashtu përfshin shërbime këshillimore për partnerin sipas kontratës nëse kjo lidhet me qëllimin kontraktual. Përpara një kontrate - gjatë fazës së inicimit të kontratës - të dhënat personale të ofruara nga subjekti tjetër kontraktues përpunohen për të përgatitur ofertat, urdhrat e blerjes dhe marrëveshjet ose për të përmbushur kërkesa të tjera të klientit potencial ose atij që lidhet me aktivitetet e shitjes. Klientët potencialë mund të kontaktohen gjatë procesit të përgatitjes së kontratës duke përdorur informacionin që ata kanë dhënë. Çdo kufizim i kërkuar nga klientët potencialë duhet të zbatohet.

C.2. Përpunimi i të Dhënave për Qëllime Reklamimi

Nëse subjekti i të dhënave kontakton F NEX për të kërkuar informacion (p.sh., kërkesë për të marrë material informues në lidhje me një produkt), përpunimi i të dhënave për të përmbushur këtë kërkesë lejohet. Masat e besnikërisë së klientit ose të reklamimit i nënshtrohen kërkesave të mëtejshme ligjore. Të dhënat personale mund të përpunohen për qëllime reklamimi ose për kërkime tregu dhe opinioni, me kusht që kjo të jetë në përputhje me qëllimin për të cilin të dhënat janë mbledhur fillimisht. Subjekti i të dhënave duhet të informohet për përdorimin e të dhënave të tij/saj për qëllime reklamimi. Nëse të dhënat mblidhen vetëm për qëllime reklamimi, zbulimi nga subjekti i të dhënave është vullnetar. Subjekti i të dhënave duhet të informohet se dhënia e të dhënave për këtë qëllim është vullnetare. Gjatë komunikimit me subjektin e të dhënave, duhet të merret pëlqimi prej tij/saj për të përpunuar të dhënat për qëllime reklamimi. Kur jep pëlqimin, subjektit të të dhënave duhet t'i jepet mundësia të zgjedhë midis formave të disponueshme të kontaktit, të tilla si posta e rregullt, email-i dhe telefoni. Nëse subjekti i të dhënave refuzon përdorimin e të dhënave të tij/saj për qëllime reklamimi, ato nuk mund të përdoren më për këto qëllime dhe duhet të bllokohen nga përdorimi për këto qëllime. Duhet të respektohet çdo kufizim tjetër nga vende të caktuara në lidhje me përdorimin e të dhënave për qëllime reklamimi.

C.3. Pëlqimi për Përpunimin e të Dhënave

Të dhënat mund të përpunohen pas pëlqimit nga subjekti i të dhënave. Përpara dhënies së pëlqimit, subjekti i të dhënave duhet të informohet për këtë Politikë të Privatësisë dhe Mbrojtjes së të Dhënave. Deklarata e pëlqimit duhet të merret me shkrim ose elektronikisht për qëllime dokumentimi.

C.4. Përpunimi i të Dhënave në Përputhje me Autorizimin Ligjor

Përpunimi i të dhënave personale lejohet gjithashtu nëse legjislacioni kombëtar e kërkon, e kërkon ose e lejon këtë. Lloji dhe shkalla e përpunimit të të dhënave duhet të jenë të nevojshme për aktivitetin e përpunimit të të dhënave të autorizuar ligjërisht dhe duhet të jenë në përputhje me dispozitat përkatëse statutore.

C.5. Përpunimi i të Dhënave në Përputhje me Interesin Legjitim

Të dhënat personale mund të përpunohen gjithashtu nëse është e nevojshme për një interes legjitim të F NEX. Interesat legjitime janë përgjithësisht të natyrës ligjore (p.sh. mbledhja e të arkëtueshmeve të papaguara) ose tregtare (p.sh. shmangia e shkeljeve të kontratës). Të dhënat personale nuk mund të përpunohen për qëllime të një interesi legjitim nëse, në raste individuale, ka prova se interesat e subjektit të të dhënave meritojnë mbrojtje dhe se kjo ka përparësi. Përpara se të përpunohen të dhënat, është e nevojshme të përcaktohet nëse ka interesa që meritojnë mbrojtje.

C.6. Përpunimi i të Dhënave Shumë të Ndjeshme

Të dhënat personale shumë të ndjeshme mund të përpunohen vetëm nëse ligji e kërkon këtë ose nëse subjekti i të dhënave ka dhënë pëlqimin e shprehur. Këto të dhëna mund të përpunohen gjithashtu nëse është e detyrueshme për të pohuar, ushtruar ose mbrojtur pretendime ligjore në lidhje me subjektin e të dhënave. Për mbrojtjen e të dhënave kontaktoni me info@f-nex.com.

C.7. Vendime Individuale të Automatizuara

Përpunimi automatik i të dhënave personale që përdoret për të vlerësuar aspekte të caktuara nuk mund të jetë baza e vetme për vendime që kanë pasoja ligjore negative ose që mund të dëmtojnë ndjeshëm subjektin e të dhënave. Subjekti i të dhënave duhet të informohet për faktet dhe rezultatet e vendimeve individuale të automatizuara dhe mundësinë për t'u përgjigjur. Për të shmangur vendimet e gabuara, një punonjës duhet të bëjë një test dhe një kontroll të besueshmërisë.

C.8. Të Dhënat e Përdoruesit dhe Interneti

Nëse të dhënat personale mblidhen, përpunohen dhe përdoren në faqet e internetit dhe në aplikacione, subjektet e të dhënave duhet të informohen për këtë në një deklaratë privatësie dhe, nëse është e aplikueshme, në informacion në lidhje me cookie-t. Deklarata e privatësisë dhe çdo informacion i cookie-t duhet të integrohen në mënyrë që të jenë të lehta për t'u identifikuar, të arritshme drejtpërdrejt dhe të disponueshme vazhdimisht për subjektet e të dhënave. Nëse profilet e përdoruesve (gjurmimi) krijohen për të vlerësuar përdorimin e faqeve të internetit dhe aplikacioneve, subjekti i të dhënave duhet të informohet gjithmonë në përputhje me rrethanat në deklaratën e privatësisë. Gjurmimi personal mund të kryhet vetëm nëse lejohet sipas ligjit kombëtar ose me pëlqimin e subjektit të të dhënave. Nëse gjurmimi përdor një pseudonim, subjektit të të dhënave duhet t'i jepet mundësia të zgjedhë të mos e bëjë këtë në deklaratën e privatësisë. Nëse faqet e internetit ose aplikacionet mund të kenë qasje në të dhënat personale në një zonë të kufizuar vetëm për përdoruesit e regjistruar, identifikimi dhe vërtetimi i subjektit të të dhënave duhet të ofrojë mbrojtje të mjaftueshme gjatë qasjes.

C.9. Zbulimi nga Pala e Tretë

F NEX nuk shet, tregton ose transferon në ndonjë mënyrë tjetër tek palët e jashtme Informacionin tuaj Personal.

Të Dhënat e Punonjësve

D.1. Përpunimi i të Dhënave për Marrëdhënien e Punësimit

Në marrëdhëniet e punësimit, të dhënat personale mund të përpunohen nëse është e nevojshme për të filluar, zbatuar dhe përfunduar marrëveshjen e punësimit. Kur fillon një marrëdhënie pune, të dhënat personale të aplikantit mund të përpunohen. Nëse kandidati refuzohet, të dhënat e tij/saj duhet të fshihen në përputhje me periudhën e kërkuar të ruajtjes, përveç nëse aplikanti ka rënë dakord të mbetet në dosje për një proces të ardhshëm përzgjedhjeje. Pëlqimi është gjithashtu i nevojshëm për të përdorur të dhënat për procese të mëtejshme aplikimi. Në marrëdhënien ekzistuese të punësimit, përpunimi i të dhënave duhet të lidhet gjithmonë me qëllimin e marrëveshjes së punësimit nëse nuk zbatohet asnjë nga rrethanat e mëposhtme për përpunimin e autorizuar të të dhënave. Nëse gjatë procedurës së aplikimit është e nevojshme të mblidhen informacione mbi një aplikant nga një palë e tretë, duhet të respektohen kërkesat e ligjeve përkatëse kombëtare së bashku me kërkesat e GDPR-së. Në rast dyshimi, duhet të merret pëlqimi nga subjektet e të dhënave. Duhet të ketë autorizim ligjor për të përpunuar të dhëna personale që lidhen me marrëdhënien e punës, por që fillimisht nuk kanë qenë pjesë e zbatimit të marrëveshjes së punës. Kjo mund të përfshijë kërkesat ligjore, rregulloret kolektive me përfaqësuesit e punonjësve, pëlqimin e punonjësit ose interesin legjitim të kompanisë.

D.2. Përpunimi i të Dhënave në Përputhje me Autorizimin Ligjor

Përpunimi i të dhënave personale të punonjësve lejohet gjithashtu nëse legjislacioni kombëtar e kërkon, e kërkon ose e autorizon këtë. Lloji dhe shkalla e përpunimit të të dhënave duhet të jetë e nevojshme për aktivitetin e përpunimit të të dhënave të autorizuar ligjërisht dhe duhet të jetë në përputhje me dispozitat përkatëse statutore. Nëse ka njëfarë fleksibiliteti ligjor, duhet të merren në konsideratë interesat e punonjësit që meritojnë mbrojtje.

D.3. Marrëveshjet Kolektive mbi Përpunimin e të Dhënave

Nëse një aktivitet përpunimi të dhënash tejkalon qëllimin e përmbushjes së një kontrate, ai mund të jetë i lejueshëm nëse autorizohet përmes një marrëveshjeje kolektive. Marrëveshjet kolektive janë marrëveshje për shkallën e pagave ose marrëveshje midis punëdhënësve dhe përfaqësuesve të punonjësve, brenda fushëveprimit të lejuar sipas ligjit përkatës të punësimit. Marrëveshjet duhet të mbulojnë qëllimin specifik të aktivitetit të synuar të përpunimit të të dhënave dhe duhet të hartohen brenda parametrave të GDPR-së.

D.4. Pëlqimi për Përpunimin e të Dhënave

Të dhënat e punonjësve mund të përpunohen me pëlqimin e personit në fjalë. Deklaratat e pëlqimit duhet të dorëzohen vullnetarisht. Pëlqimi i pavullnetshëm është i pavlefshëm. Deklarata e pëlqimit duhet të merret me shkrim ose elektronikisht për qëllime dokumentimi. Në rrethana të caktuara, pëlqimi mund të jepet me gojë, në të cilin rast duhet të dokumentohet siç duhet. Në rast të ofrimit të të dhënave të informuara dhe vullnetare nga pala përkatëse, pëlqimi mund të supozohet nëse ligjet kombëtare nuk kërkojnë pëlqim të shprehur. Përpara dhënies së pëlqimit, subjekti i të dhënave duhet të informohet në përputhje me këtë Politikë për Mbrojtjen e të Dhënave.

D.5. Përpunimi i të Dhënave në Përputhje me Interesin Legjitim

Të dhënat personale mund të përpunohen gjithashtu nëse është e nevojshme për të zbatuar një interes legjitim të F NEX. Interesat legjitime janë përgjithësisht të natyrës ligjore (p.sh. paraqitja, zbatimi ose mbrojtja kundër pretendimeve ligjore) ose financiare (p.sh. vlerësimi i kompanive). Të dhënat personale nuk mund të përpunohen bazuar në një interes legjitim nëse, në raste individuale, ka prova se interesat e punonjësit meritojnë mbrojtje. Përpara se të përpunohen të dhënat, duhet të përcaktohet nëse ka interesa që meritojnë mbrojtje. Masat e kontrollit që kërkojnë përpunimin e të dhënave të punonjësve mund të merren vetëm nëse ekziston një detyrim ligjor për ta bërë këtë ose nëse ekziston një arsye legjitime. Edhe nëse ekziston një arsye legjitime, duhet të shqyrtohet edhe proporcionaliteti i masës së kontrollit. Interesat e justifikuara të kompanisë në kryerjen e masës së kontrollit (p.sh. përputhshmëria me dispozitat ligjore dhe rregullat e brendshme të kompanisë) duhet të peshohen kundrejt çdo interesi që meriton mbrojtje që punonjësi i prekur nga masa mund të ketë në përjashtimin e saj, dhe nuk mund të kryhen nëse nuk është e përshtatshme. Interesat legjitime të kompanisë dhe çdo interes i punonjësit që meriton mbrojtje duhet të identifikohen dhe dokumentohen para se të merren masa. Për më tepër, çdo kërkesë shtesë sipas ligjit kombëtar (p.sh. të drejtat e bashkëvendosjes për përfaqësuesit e punonjësve dhe të drejtat e informacionit të subjekteve të të dhënave) duhet të merren parasysh.

D.6. Përpunimi i të Dhënave Shumë të Ndjeshme

Të dhënat personale shumë të ndjeshme mund të përpunohen vetëm në kushte të caktuara. Të dhënat shumë të ndjeshme janë të dhëna në lidhje me origjinën racore dhe etnike, bindjet politike, besimet fetare ose filozofike, anëtarësimin në sindikata dhe shëndetin dhe jetën seksuale të subjektit të të dhënave. Sipas ligjit kombëtar, kategoritë e mëtejshme të të dhënave mund të konsiderohen shumë të ndjeshme ose përmbajtja e kategorive të të dhënave mund të plotësohet ndryshe. Për më tepër, të dhënat që lidhen me një krim shpesh mund të përpunohen vetëm sipas kërkesave të veçanta sipas ligjit kombëtar. Përpunimi duhet të lejohet ose të përcaktohet shprehimisht sipas ligjit kombëtar. Përveç kësaj, përpunimi mund të lejohet nëse është e nevojshme që autoriteti përgjegjës të përmbushë të drejtat dhe detyrat e tij në fushën e ligjit të punësimit. Punonjësi gjithashtu mund të japë pëlqimin e tij të shprehur për përpunimin. Nëse ka plane për të përpunuar të dhëna shumë të ndjeshme, zyrtari i Mbrojtjes së të Dhënave duhet të informohet paraprakisht.

D.7. Vendime të Automatizuara

Nëse të dhënat personale përpunohen automatikisht si pjesë e marrëdhënies së punësimit dhe vlerësohen detaje specifike personale (p.sh. si pjesë e përzgjedhjes personale ose vlerësimit të profileve të aftësive), ky përpunim automatik nuk mund të jetë baza e vetme për vendime që do të kishin pasoja negative ose probleme të rëndësishme për punonjësin e prekur. Për të shmangur vendimet e gabuara, procesi i automatizuar duhet të sigurojë që një person fizik të vlerësojë përmbajtjen e situatës dhe që ky vlerësim të jetë baza e vendimit. Subjekti i të dhënave duhet gjithashtu të informohet për faktet dhe rezultatet e vendimeve individuale të automatizuara dhe mundësinë për t'u përgjigjur.

D.8. Telekomunikacioni dhe Interneti

Pajisjet telefonike, adresat e email-it, intraneti dhe interneti, së bashku me rrjetet e brendshme sociale, ofrohen nga kompania kryesisht për detyra të lidhura me punën. Ato janë një mjet dhe burim i kompanisë. Ato mund të përdoren brenda rregulloreve ligjore në fuqi dhe politikave të brendshme të kompanisë. Në rast të përdorimit të autorizuar për qëllime private, duhet të respektohen ligjet përkatëse kombëtare dhe ndërkombëtare, nëse është e aplikueshme. Për t'u mbrojtur nga sulmet ndaj infrastrukturës së IT-së ose përdoruesve individualë, mund të zbatohen masa mbrojtëse për lidhjet me rrjetin e F NEX që bllokojnë përmbajtjen teknikisht të dëmshme ose që analizojnë modelet e sulmit. Nuk do të ketë monitorim të përgjithshëm të komunikimeve telefonike dhe me email ose përdorimit të internetit/intranetit. Për arsye sigurie, përdorimi i pajisjeve telefonike, adresave të email-it, internetit/intranetit dhe rrjeteve të brendshme sociale mund të regjistrohet për një periudhë të përkohshme. Vlerësimet e këtyre të dhënave nga një person specifik mund të bëhen vetëm në një rast konkret dhe të justifikuar të dyshimit për shkelje të ligjeve ose politikave të F NEX. Vlerësimet mund të kryhen vetëm nga departamentet hetuese, duke siguruar që të përmbushet parimi i proporcionalitetit. Ligjet përkatëse kombëtare duhet të respektohen në të njëjtën mënyrë si rregulloret e GDPR-së.

Transmetimi i të Dhënave Personale

Transmetimi i të Dhënave Personale jashtë ose brenda F NEX i nënshtrohet kërkesave të autorizimit për përpunimin e të dhënave personale. Marrësi i të dhënave duhet të jetë i detyruar t'i përdorë të dhënat vetëm për qëllimet e përcaktuara. Në rast se të dhënat transmetohen te një marrës në një vend të tretë, ai marrës duhet të jetë dakord të mbajë një nivel mbrojtjeje të të dhënave ekuivalent me këtë Politikë të Privatësisë dhe Mbrojtjes së të Dhënave. Kjo nuk zbatohet nëse transmetimi bazohet në një detyrim ligjor. Nëse të dhënat merren nga një vend i tretë, F NEX duhet të sigurojë që të dhënat mund të përdoren për qëllimin e synuar dhe, kur kërkohet, të bashkëpunojë me çdo kërkesë të bërë nga autoriteti mbikëqyrës përkatës në lidhje me përpunimin e të dhënave të transmetuara.

Përpunimi i të Dhënave të Kontratës

Përpunimi i të dhënave në emër të klientit do të thotë që një ofrues punësohet për të përpunuar të dhëna personale, pa iu caktuar përgjegjësia për procesin përkatës të biznesit. Në këto raste, një marrëveshje për Përpunimin e të Dhënave në emër të klientit duhet të lidhet me ofruesit e jashtëm. Klienti mban përgjegjësi të plotë për kryerjen e saktë të përpunimit të të dhënave. Ofruesit mund të përpunojnë të dhëna personale vetëm sipas udhëzimeve të klientit. Gjatë lëshimit të porosisë, duhet të përmbushen kërkesat e mëposhtme; departamenti që bën porosinë duhet të sigurojë që ato të përmbushen.

1. Ofruesi duhet të zgjidhet bazuar në aftësinë e tij për të mbuluar masat mbrojtëse teknike dhe organizative të kërkuara.
2. Porosia duhet të bëhet me shkrim. Udhëzimet mbi përpunimin e të dhënave dhe përgjegjësitë e klientit dhe ofruesit duhet të dokumentohen.
3. Duhet të merren në konsideratë standardet kontraktuale për mbrojtjen e të dhënave të ofruara nga Zyrtari i Mbrojtjes së të Dhënave.

4. Përpara se të fillojë përpunimi i të dhënave, klienti duhet të jetë i sigurt se ofruesi do t'i përmbushë detyrimet. Një ofrues mund të dokumentojë përputhshmërinë e tij me kërkesat e sigurisë së të dhënave, në veçanti duke paraqitur certifikim të përshtatshëm. Në varësi të rrezikut të përpunimit të të dhënave, shqyrtimet duhet të përsëriten rregullisht gjatë afatit të kontratës.
5. Në rast të përpunimit të kontratave ndërkufitare, duhet të përmbushen kërkesat përkatëse kombëtare për zbulimin e të dhënave personale jashtë vendit. Në veçanti, të dhënat personale nga Zona Ekonomike Evropiane mund të përpunohen në një vend të tretë vetëm nëse ofruesi mund të provojë se ka standarde të mbrojtjes së të dhënave ekuivalente me këtë politikë të Mbrojtjes së të Dhënave.

Mjete të përshtatshme mund të jenë:

1. Marrëveshjet mbi klauzolat standarde të kontratave të BE-së për përpunimin e kontratave në vendet e treta me ofruesin dhe çdo nënkontraktor.
2. Pjesëmarrja e ofruesit në një sistem certifikimi të akredituar nga BE-ja për ofrimin e një niveli të mjaftueshëm të mbrojtjes së të dhënave.
3. Njohja e rregullave të detyrueshme të korporatës së ofruesit për të krijuar një nivel të përshtatshëm të mbrojtjes së të dhënave nga autoritetet mbikëqyrëse përgjegjëse për mbrojtjen e të dhënave.

Të Drejtat e Subjektit të të Dhënave

Çdo subjekt i të dhënave ka të drejtat e mëposhtme. Kërkesat duhet të trajtohen menjëherë nga njësia përgjegjëse dhe nuk mund të paraqesin ndonjë disavantazh për subjektin e të dhënave.

1. Subjekti i të dhënave mund të kërkojë informacion se cilat të dhëna personale që lidhen me të janë ruajtur, si janë mbledhur të dhënat dhe për çfarë qëllimi. Nëse ka të drejta të mëtejshme për të parë dokumentet e punëdhënësit (p.sh. dosjet e personelit) për marrëdhënien e punës sipas ligjeve përkatëse të punësimit, këto do të mbeten të paprekura.
2. Nëse të dhënat personale u transmetohen palëve të treta, duhet të jepet informacion në lidhje me identitetin e marrësit ose kategorinë e marrësve.
3. Nëse të dhënat personale janë të pasakta ose të paplota, subjekti i të dhënave mund të kërkojë që ato të korrigjohen ose plotësohen.
4. Subjekti i të dhënave mund të kundërshtojë përpunimin e të dhënave të tij/saj për qëllime reklamimi ose kërkimi të tregut/opinionit. Të dhënat duhet të bllokohen nga këto lloje përdorimi.
5. Subjekti i të dhënave mund të kërkojë fshirjen e të dhënave të tij/saj nëse përpunimi i të dhënave të tilla nuk ka bazë ligjore ose nëse baza ligjore ka pushuar së zbatuari. E njëjta gjë vlen edhe nëse qëllimi i përpunimit të të dhënave ka skaduar ose ka pushuar së zbatuari për arsye të tjera. Duhet të respektohen periudhat ekzistuese të ruajtjes dhe interesat në konflikt që meritojnë mbrojtje.
6. Subjekti i të dhënave në përgjithësi ka të drejtë të kundërshtojë përpunimin e të dhënave të tij/saj dhe kjo duhet të merret parasysh nëse mbrojtja e interesave të tij/saj ka përparësi mbi interesin e kontrolluesit të të dhënave për shkak të një situate të veçantë personale. Kjo nuk zbatohet nëse një dispozitë ligjore kërkon që të dhënat të përpunohen.

Konfidencialiteti i Përpunimit

Të dhënat personale i nënshtrohen sekretit të të dhënave. Çdo mbledhje, përpunim ose përdorim i paautorizuar i të dhënave të tilla nga punonjësit është i ndaluar. Çdo përpunim i të dhënave i ndërmarrë nga një punonjës, të cilin ai/ajo nuk është autorizuar ta kryejë si pjesë e detyrave të tij/saj legjitime, është i paautorizuar. Zbatohet parimi "nevojë për të ditur". Punonjësit mund të kenë qasje në informacionin personal vetëm kur është e përshtatshme për llojin dhe fushëveprimin e detyrës në fjalë. Kjo kërkon një ndarje dhe ndarje të kujdesshme, si dhe zbatim të roleve dhe përgjegjësive. Punonjësve u ndalohet të përdorin të dhënat personale për qëllime private ose tregtare, t'ua zbulojnë ato personave të paautorizuar ose t'i bëjnë të disponueshme në ndonjë mënyrë tjetër. Mbikëqyrësit duhet t'i informojnë punonjësit e tyre në fillim të marrëdhënies së punës në lidhje me detyrimin për të mbrojtur sekretin e të dhënave. Ky detyrim mbetet në fuqi edhe pas përfundimit të punësimit.

Siguria e Përpunimit

Të dhënat personale duhet të mbrohen nga qasja e paautorizuar dhe përpunimi ose zbulimi i paligjshëm, si dhe humbja, modifikimi ose shkatërrimi aksidental. Kjo vlen pavarësisht nëse të dhënat përpunohen elektronikisht apo në formë letre. Para futjes së metodave të reja të përpunimit të të dhënave, veçanërisht sistemeve të reja të IT-së, duhet të përcaktohen dhe zbatohen masa teknike dhe organizative për mbrojtjen e të dhënave personale. Këto masa duhet të bazohen në gjendjen e mëparshme, rreziqet e përpunimit dhe nevojën për të mbrojtur të dhënat (të përcaktuara nga procesi për klasifikimin e informacionit). Masat teknike dhe organizative për mbrojtjen e të dhënave personale janë pjesë e Sistemit të Integruar të Menaxhimit të Kompanisë dhe duhet të përshtaten vazhdimisht me zhvillimet teknike dhe ndryshimet organizative.

Kontrolli/Auditimet e Mbrojtjes së të Dhënave

Pajtueshmëria me politikën e Mbrojtjes së të Dhënave dhe ligjet përkatëse të mbrojtjes së të dhënave/GDPR-në kontrollohet rregullisht me auditime të mbrojtjes së të dhënave dhe kontrolle të tjera. Kryerja e këtyre kontrolleve është përgjegjësi e Zyrtarit të Mbrojtjes së të Dhënave, koordinatorëve të mbrojtjes së të dhënave dhe njësive të tjera të kompanisë me të drejta auditimi ose auditorëve të jashtëm të punësuar. Rezultatet e kontrolleve të mbrojtjes së të dhënave duhet t'i raportohen Zyrtarit të Mbrojtjes së të Dhënave. F NEX duhet të informohet për rezultatet parësore si pjesë e detyrave përkatëse të raportimit. Me kërkesë, rezultatet e kontrolleve të mbrojtjes së të dhënave do t'i vihen në dispozicion autoritetit përgjegjës të mbrojtjes së të dhënave. Autoriteti përgjegjës i mbrojtjes së të dhënave mund të kryejë kontrollet e veta të pajtueshmërisë me rregulloret e kësaj politike, siç lejohet sipas ligjit kombëtar.

Incidente të të Dhënave

Të gjithë punonjësit duhet të informojnë menjëherë mbikëqyrësin e tyre, koordinatorin e mbrojtjes së të dhënave ose Zyrtarin e Mbrojtjes së të Dhënave për rastet e shkeljeve të kësaj Politike të Privatësisë dhe Mbrojtjes së të Dhënave ose rregulloreve të tjera mbi mbrojtjen e të dhënave personale (incidente të mbrojtjes së të dhënave). Menaxheri përgjegjës për funksionin ose njësinë është i detyruar të informojë menjëherë Zyrtarin e Mbrojtjes së të Dhënave për incidentet e mbrojtjes së të dhënave. F NEX është i detyruar t'i raportojë këto incidente autoriteteve mbikëqyrëse dhe individit të prekur brenda 72 orëve nga një shkelje në rast të:

1. Transmetim i papërshtatshëm i të dhënave personale te palët e treta.
2. Qasje e papërshtatshme nga palët e treta në të dhënat personale, ose
3. Humbja e të dhënave personale.

Raportet e kërkuara të kompanisë (Menaxhimi i Incidenteve) duhet të bëhen menjëherë në mënyrë që të mund të përmbushen çdo detyrim raportimi sipas GDPR-së dhe ligjit kombëtar.

Përgjegjësitë dhe Sanksionet

Organet ekzekutive të F NEX janë përgjegjëse për përpunimin e të dhënave në fushën e tyre të përgjegjësisë. Prandaj, ata janë të detyruar të sigurojnë që të përmbushen kërkesat ligjore dhe ato të përfshira në Politikën e Mbrojtjes dhe Privatësisë së të Dhënave, për mbrojtjen e të dhënave. Stafi drejtues është përgjegjës për të siguruar që masat organizative, të burimeve njerëzore dhe teknike janë në vend, në mënyrë që çdo përpunim i të dhënave të kryhet në përputhje me mbrojtjen e të dhënave. Pajtueshmëria me këto kërkesa është përgjegjësi e punonjësve përkatës. Nëse agjencitë zyrtare kryejnë kontrolle të mbrojtjes së të dhënave, Zyrtari i Mbrojtjes së të Dhënave duhet të informohet menjëherë. Zyrtari i Mbrojtjes së të Dhënave është personi i kontaktit në vend për mbrojtjen e të dhënave. Zyrtari i Mbrojtjes së të Dhënave duhet t'i njohë punonjësit me përmbajtjen e politikave të mbrojtjes së të dhënave. Menaxhmenti përkatës është i detyruar të ndihmojë Zyrtarin e Mbrojtjes së të Dhënave në përpjekjet e tij. Departamentet përgjegjëse për proceset dhe projektet e biznesit duhet ta informojnë DPO-në në kohën e duhur për përpunimin e ri të të dhënave personale. Për planet e përpunimit të të dhënave që mund të paraqesin një rrezik të veçantë për të drejtat individuale të subjekteve të të dhënave, Zyrtari i Mbrojtjes së të Dhënave duhet të informohet para se të fillojë përpunimi. Kjo vlen veçanërisht për të dhënat personale jashtëzakonisht të ndjeshme. Menaxherët duhet të sigurohen që punonjësit e tyre të jenë të trajnuar mjaftueshëm në mbrojtjen e të dhënave. Përpunimi i papërshtatshëm i të dhënave personale, ose shkelje të tjera të ligjeve për mbrojtjen e të dhënave, mund të ndiqen penalisht në shumë vende dhe të rezultojnë në kërkesa për kompensim dëmi. Shkeljet për të cilat janë përgjegjës punonjës individualë mund të çojnë madje edhe në sanksione. Për mbrojtjen e të dhënave kontaktoni me info@f-nex.com.