Euroopa Komisjon

GDPR – uued võimalused ja kohustused

Mida peab iga ettevõtja teadma ELi isikuandmete kaitse üldmääruse kohta?

Õigus- ja tarbijaküsimused

Printed by Bietlot in Belgium

Luxembourg: Euroopa Liidu Väljaannete Talitus, 2018

Print	ISBN 978-92-79-79447-6	doi:10.2838/994121	DS-01-18-082-ET-C
PDF	ISBN 978-92-79-79438-4	doi:10.2838/010396	DS-01-18-082-ET-N

SISUKORD

1.

ÄRIVÕIMALUS

Isikuandmete kaitse üldmäärus (inglise k *General Data Protection Regulation*, GDPR) reguleerib isikuandmete töötlemist ja haldamist ettevõtetes. 25. maist 2018 kõigile ettevõtetele ja organisatsioonidele (nt haiglad, avaliku sektori asutused jne) kohaldatav üldmäärus kujutab endast ELi andmekaitse eeskirjade suurimat muutust 20 aasta jooksul.

GDPRi alusel on inimeste isikuandmed rohkem nende kontrolli all, samuti muudab see õiguskeskkonna ettevõtjate jaoks märkimisväärselt ühtlasemaks. Seda seetõttu, et GDPRiga kehtestatakse kogu ELis ühtne andmekaitsealane õigusraamistik. Teisisõnu reguleeritakse seda valdkonda nüüd kogu ELis üheainsa määrusega, selle asemel, et igas riigis oleksid omaenda õigusaktid andmekaitse kohta. Seega ei pea mitmes riigis tegutsev ettevõtja enam järgima mitut ja sageli erinevat õigusakti. Selle asemel peavad nad järgima ainult GDPRi sätteid, osutades teenuseid kõikjal ELis.

Mis kasu on GDPRist Teie ettevõttele?

- **Üks liit, üks seadus:** ühtsed eeskirjad muudavad ELis tegutsemise ettevõtjate jaoks lihtsamaks ja odavamaks.
- **Ühtne kontaktpunkt:** enamasti peavad ettevõtjad suhtlema ainult ühe andmekaitseasutusega.
- **Euroopa reeglid Euroopa pinnal:** ettevõtjad, kelle tegevuskoht on väljaspool ELi, peavad ELis inimestele kaupu müües või teenuseid osutades järgima samu eeskirju nagu Euroopa ettevõtjad.
- **Riskipõhine lähenemisviis:** GDPR ei näe ette kõigile ühtemoodi koormavaid kohustusi, vaid neid kohandatakse vastavalt riskitasemele.
- **Uuendusteks sobivad eeskirjad:** GDPR on tehnoloogiliselt neutraalne.

Asi on usalduses

Isikuandmete kaitse on inimestele tähtis murekoht. Seepärast ei usalda nad ikka veel eriti digikeskkonda. Eurobaromeetri uuring näitas:

- kümnest inimesest kaheksa leiavad, et nende isikuandmed ei ole täielikult enda kontrolli all;
- kümnest inimesest kuus ütlevad, et nad ei usalda veebiettevõtteid;
- üle 90% eurooplastest tahavad, et samad andmekaitseõigused kehtiksid kõigis ELi riikides.

GDPR pakub Teie ettevõttele uue võimaluse võita tarbija usaldust isikuandmete riskipõhise haldamise kaudu.

„Ettevõtjad, kes ei kaitse piisavalt inimeste isikuandmeid, riskivad tarbija usalduse kaotamisega, kuid see on hädavajalik, et julgustada inimesi uusi tooteid ja teenuseid kasutama.”

2.

ISIKUANDMETE KAITSE ÜLDMÄÄRUSE SELGITUS

Kas GDPR kehtib ka minu kohta?

Üldiselt kehtib GDPR ***igale*** ettevõttele, kes

töötleb isikuandmeid automatiseeritult või **käsitsi** (kui andmed on teatavate kriteeriumide kohaselt korrastatud).

Isegi kui Teie ettevõte töötleb andmeid ainult teiste ettevõtete nimel, peate neid eeskirju järgima.

GDPRi kohaldatakse, kui

- Teie ettevõte töötleb isikuandmeid ja tegutseb ELis, sõltumata andmete tegelikust töötlemiskohast, või
- Teie ettevõtte tegevuskoht asub väljaspool ELi, kuid müüte kaupu, osutate teenuseid või jälgite inimeste käitumist ELis.

Mis on isikuandmed?

Isikuandmed on mis tahes teave üheselt tuvastatud või tuvastatava elava üksikisiku kohta. Nende hulka võivad kuuluda:

- nimi;
- aadress ja telefoninumber;
- asukoht;
- terviseandmed;
- teave sissetulekute ja pangakonto kohta;
- kultuurilised eelistused
- ja palju muud.

Kui isikuandmed on muudetud mitteidentifitseeritavaks või pseudonümiseeritud, kuid neid saab siiski kasutada isiku uuesti tuvastamiseks, kuuluvad need samuti GDPRi reguleerimisalasse. Ent kui isikuandmed on muudetud pöördumatult anonüümseks sellisel viisil, et inimest ei ole enam võimalik tuvastada, ei loeta neid enam isikuandmeteks ja seetõttu ei kuulu need GDPRi reguleerimisalasse.

GDPR on ka tehnoloogiliselt neutraalne, mis tähendab, et see kaitseb isikuandmeid sõltumata nende andmete säilitamise viisist ja kasutatavast tehnoloogiast. Sõltumata sellest, kas Teie ettevõte töötleb ja säilitab isikuandmeid keerulise IT-süsteemi abil või paberil, kehtib GDPR siiski ka Teie puhul.

„Sõltumata sellest, kas Teie ettevõte töötleb ja säilitab isikuandmeid keerulise IT-süsteemi abil või paberil, kehtib GDPR siiski ka Teie puhul.”

Olge eriti ettevaatlik isikuandmete tundlike eriliikidega

Kui Teie kogutavate isikuandmete hulka kuulub teavet inimese tervise, rassi, seksuaalse sättumuse, usu, poliitiliste tõekspidamiste või ametiühingusse kuulumise kohta, loetakse neid andmeid tundlikeks. Teie ettevõte tohib neid andmeid töödelda ainult eritingimustel ja võimalik, et peate rakendama lisakaitsemeetmeid, nagu krüpteerimist.

Milles seisneb isikuandmete töötlemine?

GDPRi kohaselt hõlmab isikuandmete töötlemise määratlus näiteks isikuandmete kogumist, kasutamist ja kustutamist.

Kas Te valvate oma ruume valvekaameratega? Kas teete ettevõtluse eesmärgil päringuid andmebaasidest, milles on isikuandmeid? Kas saadate e-posti reklaamiks?

Kas kustutate töötajate digitaalseid dokumente või purustate paberdokumente? Kas postitate inimese fotosid oma veebisaidile või suhtlusmeedia kanalitesse?

Kui vastasite jaatavalt kasvõi ühele neist küsimustest, siis töötleb Teie ettevõte kindlasti isikuandmeid.

Kuidas aitab GDPR kulusid vähendada?

GDPR arvestab ettevõtjate vajadustega. Näiteks on selle määruse eesmärk kõrvaldada haldusnõudeid, et vähendada kulusid ja muuta halduskoormus minimaalseks.

- **Ei mingit etteteatamist enam**: reformiga kaotatakse enamik järelevalveasutustele etteteatamisi koos nendega seotud kuludega.
- **Andmekaitseametnikud**: ettevõtjad peavad eelkõige määrama andmekaitseametniku, kui nende põhitegevus on seotud tundlike isikuandmete ulatusliku töötlemisega või inimeste ulatusliku, korrapärase ja süstemaatilise jälgimisega. Avaliku sektori asutused on kohustatud määrama andmekaitseametniku.
- **Andmekaitsealane mõjuhinnang**: ettevõtjad on kohustatud tegema andmekaitsealase mõjuhinnangu ainult juhul, kui kavandatava andmetöötlustegevusega kaasneb suur oht inimeste õigustele ja vabadustele.
- **Arvestuse pidamine**: kuni 250 töötajaga ettevõtetes ei ole vaja arvestust pidada, välja arvatud juhul, kui andmetöötlus ei ole juhuslik või hõlmab tundlikke andmeid.

„Selle määruse eesmärk on kõrvaldada haldusnõudeid, et vähendada kulusid ja muuta halduskoormus minimaalseks.”

3.

TEIE KOHUSTUSED ISIKUANDMETE KAITSE ÜLDMÄÄRUSE KOHASELT

GDPR paneb kogu ELis ettevõtjatele otsesed kohustused seoses andmetöötlusega. GDPRi kohaselt tohib ettevõtja töödelda isikuandmeid ainult teatavatel tingimustel. Näiteks peab töötlemine olema õiglane ja läbipaistev, kindlaksmääratud õiguspärasel eesmärgil ja piiratud selle eesmärgi täitmiseks vajalike andmetega. Samuti peab see toimuma ühel järgmistest juriidilistest alustest:

- asjaomase isiku **nõusolekul**;
- vastavalt **lepingulistele kohustustele** Teie ja selle inimese vahel;
- **juriidilise kohustuse** täitmiseks;
- inimese **eluliste huvide** kaitsmiseks;
- **üldiste huvidega seotud ülesande** täitmiseks;
- seoses Teie ettevõtte **õigustatud huviga**, kuid enne tuleb kontrollida, et see ei mõjutaks tõsiselt isiku, kelle andmeid Te töötlete, põhiõigusi ja -vabadusi. Kui tema õigused kaaluvad üles Teie huvid, siis ei saa Te neid andmeid töödelda.

Tähelepanu keskpunktis on isikuandmete kasutamiseks nõusoleku saamine

GDPRis on ettenähtud ranged eeskirjad nõusoleku alusel töötlemisele. Nende eeskirjade eesmärk on tagada, et inimesed mõistaksid, millega nad nõustuvad. See tähendab, et nõusolek peab olema selges ja lihtsas keeles esitatud taotlusega **vabatahtlikult antud, konkreetne, teadlik** ja **ühemõtteline**. Peale selle tuleks nõusolek anda **selge kinnitusena**, näiteks lahtri märgistamisega veebisaidil või vormi allkirjastamisega.

Kui töötlete nõusoleku alusel **lapse** isikuandmeid, siis on vajalik ka lapsevanema nõusolek. Erinevates riikides võib sellega seotud vanusepiir olla 13–16 aastat ja seetõttu tuleks tutvuda konkreetse riigi õigusega.

Pidage meeles! Kui keegi annab nõusoleku oma isikuandmete töötlemiseks, siis saate neid andmeid töödelda ainult sellel eesmärgil, mille kohta nõusolek anti. Lisaks peate andma isikule võimaluse oma nõusolek tagasi võtta.

Tehke kindlaks oma roll ja vastutus

Kui olete kindlaks teinud, et GDPRi kohaldatakse ka Teie tegevusele, ja selles esineb isikuandmete töötlemist, siis järgmise sammuna tuleks kindlaks määrata oma roll.

Andmekaitse eeskirjades tehakse vahet vastutaval ja volitatud töötlejal: mõlemal on erinevad kohustused. Vastutav töötleja määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid, aga volitatud töötleja ainult töötleb isikuandmeid vastutava töötleja nimel. See ei tähenda siiski, et volitatud töötleja saaks vastutava töötleja selja taha pugeda.

GDPRis nõutakse, et vastutav töötleja kaasaks ainult sellise volitatud töötleja, kes pakub piisavaid tagatisi. Need tagatised peaksid olema märgitud vastutava ja volitatud töötleja vahel sõlmitud kirjalikku lepingusse. Selles lepingus peab olema ka mitu kohustuslikku sätet, muuhulgas tuleb näiteks sätestada, et volitatud töötleja töötleb isikuandmeid ainult vastutava töötleja dokumenteeritud juhiste alusel.

Kohustused, mis kaitsevad inimeste õigusi

GDPRis on ettenähtud mitu kohustust, mille eesmärk on kaitsta inimeste õigust hoida oma isikuandmed enda kontrolli all.

Teie kohustus: anda läbipaistvat teavet

Ettevõtjad peavad andma inimestele teavet selle kohta, kes mida töötleb ja milleks. Selle teabe hulgas peab selgelt märkima vähemalt,

- kes Te olete;
- miks Te neid andmeid töötlete;
- mis on selle juriidiline alus;
- kes neid andmeid saab (kui on asjakohane).

Teatud juhtudel tuleb selle teabe hulgas märkida ka järgmist:

- andmekaitseametniku kontaktandmed;
- õigustatud huvi (kui töötlemise juriidiline alus on õigustatud huvi);
- andmete väljaspool ELi asuvasse riiki edastamise alus;
- kui kaua neid andmeid säilitatakse;
- inimese andmekaitsealased õigused (st juurdepääsu, parandamise, kustutamise, piiramise, vastuväidete esitamise, ülekantavuse õigus jne);
- kuidas saab nõusoleku tagasi võtta (kui nõusolek on töötlemise juriidiline alus);
- kas nende andmete esitamine on õigusaktist või lepingust tulenev kohustus;
- automatiseeritud otsuste korral teave kasutatava loogika ning sellise otsuse tähtsuse ja tagajärgede kohta.

„Ettevõtjad peavad andma inimestele teavet selle kohta, kes mida töötleb ja milleks.”

Teie kohustus: juurdepääsu ja ülekantavuse õigus

Inimestel on õigus taotleda tasuta juurdepääsu oma isikuandmetele ja seda juurdepääsetaval kujul. Sellise taotluse saamisel tuleb Teil

- teatada sellele isikule, kas Te töötlete tema isikuandmeid;
- jagada teavet töötlemise kohta (nt eesmärgid, asjaomaste isikuandmete liigid, tema andmete vastuvõtjad jne);
- esitada koopia teda käsitlevatest isikuandmetest töödeldavate andmete hulgas.

Kui töötlemine toimub nõusoleku või lepingu alusel, võib see isik lisaks paluda oma isikuandmed talle tagastada või kanda üle teisele ettevõtjale. Seda nimetatakse andmete ülekantavuse õiguseks. Need andmed tuleb esitada laialdaselt kasutataval masinloetaval kujul.

Kuigi need kaks õigust on tihedalt seotud, on need siiski kaks täiesti eraldi õigust. Seetõttu peate tegema kindlaks, et neid kahte õigust ei ole segi aetud, ja vastavalt sellele teavitama ka seda isikut.

Teie kohustus: kustutamise õigus (õigus olla unustatud)

Teatavatel juhtudel võivad inimesed taotleda, et vastutav töötleja kustutaks nende isikuandmed, näiteks kui neid andmeid ei vajata enam töötlemise eesmärgi täitmiseks. Teie ettevõte ei ole siiski kohustatud inimeste taotlusi täitma, kui

- töötlemine on vajalik sõna- ja teabevabaduse õiguse teostamiseks;
- Te peate neid isikuandmeid hoidma seadusjärgse kohustuse täitmiseks;
- nende isikuandmete hoidmine on teistel põhjustel avalikes huvides, nagu rahvatervise ja teadus- või ajaloouuringute eesmärgil;
- Teil on vaja neid isikuandmeid hoida õigusnõude koostamiseks.

Teie kohustus: parandamise ja vastuväite esitamise õigused

Kui kellegi arvates on ta isikuandmed ebaõiged, ebatäielikud või ebatäpsed, siis on tal õigus nõuda nende põhjendamatu viivituseta parandamist või täiendamist.

Samuti võidakse alati esitada vastuväiteid oma isikuandmete töötlemisele mingil konkreetsel eesmärgil, kui Teie ettevõte töötleb neid oma õigustatud huvi alusel või avalikes huvides oleva ülesande täitmiseks. Te peate nende isikuandmete töötlemise lõpetama, välja arvatud juhul, kui Teie õigustatud huvi kaalub üles selle isiku huvid. Inimene võib nõuda ka oma isikuandmete töötlemise piiramist, kuni tehakse kindlaks, kas Teie õigustatud huvi kaalub üles tema huvi. Otseturunduse korral olete siiski alati kohustatud inimese taotluse saamisel tema isikuandmete töötlemise lõpetama.

Hoiatus automatiseeritud otsuste tegemise ja profiilianalüüsi kohta

Inimestel on õigus, et nende kohta ei võetaks otsust, mis põhineb üksnes automatiseeritud töötlusel. Sellel reeglil on siiski erandid, näiteks juhul, kui isik on andnud selgesõnalise nõusoleku automatiseeritud otsuste tegemiseks. Välja arvatud juhul, kui automatiseeritud otsuse tegemine põhineb õigusaktil, peab Teie ettevõte

- teavitama inimest automatiseeritud otsuste tegemisest;
- andma talle õiguse lasta automatiseeritult tehtud otsus inimesel üle vaadata;
- andma talle võimaluse esitada vastuväide automatiseeritult tehtud otsusele.

Näiteks kui pank teeb automatiseeritult otsuse, kas anda konkreetsele inimesele laenu või mitte, tuleb sellele inimesele teatada automatiseeritult tehtud otsusest ning anda talle võimalus otsust vaidlustada ja taotleda inimese sekkumist.

Riskipõhised kohustused

Lisaks kohustustele, MILLE eesmärk on kaitsta konkreetseid õigusi, nähakse GDPRis ette mitu kohustust, mille rakendamine sõltub riskist.

Teie kohustus: määrata andmekaitseametnik

Andmekaitseametniku ülesanne on jälgida, et Te järgite GDPRi nõudeid. Andmekaitseametniku üks põhiülesandeid on teavitada ja nõustada tegelikult isikuandmeid töötlevaid töötajaid seoses nende kohustustega. Andmekaitseametnik teeb koostööd andmekaitseasutusega, olles kontaktpunktiks inimestele ja andmekaitseasutusele.

Teie ettevõte peab määrama andmekaitseametniku, kui

- tegelete inimeste regulaarse ja süstemaatilise järelevalvega või töötlete isikuandmete eriliike;
- selline töötlemine on teie põhitegevus ja
- teete seda ulatuslikult.

Näiteks kui töötlete isikuandmeid, et inimeste veebikäitumise põhjal suunata otsingumootorite kaudu reklaami, peab Teil GDPRi kohaselt olema andmekaitseametnik. Aga kui saadate kord aastas oma klientidele reklaami, ei pea Teil andmekaitseametnikku olema. Samamoodi ei ole tõenäoliselt andmekaitseametnikku vaja, kui olete arst, kes kogub andmeid patsientide tervise kohta. Ent kui töötlete geneetikat ja tervist puudutavaid andmeid haigla jaoks, siis on andmekaitseametnik nõutav.

Teie kohustus: lõimitud ja vaikimisi andmekaitse

GDPRis võetakse kasutusele kaks uut põhimõtet: lõimitud ja vaikimisi andmekaitse.

Lõimitud andmekaitse aitab tagada, et ettevõtja võtaks andmekaitset arvesse juba uue isikuandmete töötlemisviisi kavandamise varases järgus. Selle põhimõtte kohaselt peab vastutav töötleja rakendama kõiki tehnilisi ja korralduslikke meetmeid, mis on vajalikud andmekaitsepõhimõtete rakendamiseks ja inimeste õiguste kaitseks. Nende meetmete hulka võib näiteks kuuluda pseudonümiseerimine.

Lõimitud andmekaitse viib eraelu puutumatuse riskid miinimumini ja suurendab usaldust. Seades andmekaitse uute kaupade või teenuste väljatöötamisel esikohale, saab võimalikke andmekaitsega seotud probleeme juba varases järgus vältida. Lisaks aitab selline teguviis suurendada andmekaitsealast teadlikkust ettevõtte kõigis osakondades ja tasanditel.

Vaikimisi andmekaitse tähendab seda, et Teie ettevõte seab vaikesätteks alati sätte, mis kaitseb kõige paremini eraelu puutumatust. Näiteks kui saab valida kahe eraelu puutumatust käsitleva sätte vahel ja üks neist takistab teiste juurdepääsu isikuandmetele, tuleb seda kasutada vaikesättena.

„Lõimitud andmekaitse viib eraelu puutumatuse riskid miinimumini ja suurendab usaldust.”

„Vaikimisi andmekaitse tähendab seda, et Teie ettevõte seab vaikesätteks alati sätte, mis kaitseb kõige paremini eraelu puutumatust.”

Teie kohustus: nõuetekohane teatamine isikuandmetega seotud rikkumise korral

Isikuandmetega seotud rikkumine leiab aset siis, kui isikuandmed, mille eest Teie vastutate, avalikustatakse juhuslikult või ebaseaduslikult loata vastuvõtjatele, tehakse ajutiselt kättesaamatuks või neid muudetakse.

Ettevõtjale on eriti tähtis rakendada asjakohaseid tehnilisi ja korralduslikke meetmeid võimalike isikuandmetega seotud rikkumiste vältimiseks. Kui isikuandmetega seotud rikkumine leiab siiski aset ning see kujutab ohtu üksikisiku õigustele ja vabadustele, peate teatama sellest oma andmekaitseasutusele 72 tunni jooksul pärast rikkumisest teadasaamist.

Sõltuvalt sellest, kas isikuandmetega seotud rikkumine kujutab asjaomastele *suurt* ohtu, võib ettevõtja olla kohustatud teatama ka kõigile inimestele, keda see rikkumine mõjutab.

Kas edastate isikuandmeid väljapoole ELi?

GDPRi kohaldatakse Euroopa Majanduspiirkonnas (EMP), kuhu kuuluvad kõik ELi liikmesriigid, Island, Liechtenstein ja Norra. Kui isikuandmeid edastatakse väljapoole EMPd, liigub GDPRi alusel ettenähtud kaitse andmetega kaasa. See tähendab, et andmete välismaale eksportimiseks peavad ettevõtjad kindlustama teatavate kaitsemeetmete rakendamise.

GDPRis on ette nähtud mitmekülgsed vahendid andmete edastamiseks kolmandatesse riikidesse. GDPRi kohaselt on selline edastamine lubatav,

1. kui EL loeb kõnealuse riigi kaitsetaseme piisavaks või
2. kui Teie ettevõte astub vajalikke samme asjakohaste kaitsemeetmete rakendamiseks, näiteks lisades konkreetsed andmekaitseklauslid väljaspool Euroopat asuvasse riiki isikuandmete importijaga sõlmitud lepingusse, või
3. kui Teie ettevõte toetub edastamisel konkreetsetele alustele (nn eranditele), näiteks isiku nõusolekule.

Lisateavet rahvusvahelise andmeedastuse korral kohaldatavate eeskirjade kohta leiate Euroopa Komisjoni teatisest isikuandmete vahetamise ja kaitsmise kohta globaliseerunud maailmas: http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52017DC0007&from=ET

Kas peate tegema andmekaitsealase mõjuhinnangu?

Andmekaitsealane mõjuhinnang tuleb teha alati, kui kavandatud töötlemise tagajärjel tekib tõenäoliselt suur oht inimeste õigustele ja vabadustele. Seda võib esineda näiteks uue tehnoloogia kasutamisel.

GDPRi kohaselt esineb selline suur oht vähemalt järgmistel juhtudel:

- automatiseeritud töötlemise ja profiilianalüüsi mehhanismide kasutamine süstemaatiliselt ja ulatuslikult inimeste kohta hinnangute andmiseks;
- avalike alade ulatuslik süstemaatiline jälgimine (nt valvekaamerate abil);
- tundlike andmete (nt terviseandmete) ulatuslik töötlemine.

Andmekaitsealase mõjuhinnangu eesmärk on teha kindlaks võimalikke ohte inimeste õigustele ja vabadustele enne isikuandmete töötlemise alustamist ja enne ohtude tegelikuks saamist. Ohtude ennetava leevendamise abil saab kahjusid vältida ja kulud minimaalseks viia.

Kui andmekaitsealases mõjuhinnangus viidatud meetmete abil ei saa kõiki kindlakstehtud suuri ohte kõrvaldada, tuleb enne kavandatud andmetöötluse teostamist pidada nõu andmekaitseasutusega.

„Andmekaitsealane mõjuhinnang tuleb teha alati, kui kavandatud töötlemise tagajärjel tekib tõenäoliselt suur oht inimeste õigustele ja vabadustele.”

Mida Te peate tegema?

Taotlustele vastama

Kui Teie ettevõte saab taotluse isikult, kes soovib oma õigusi kasutada, peaksite sellele taotlusele vastama põhjendamatu viivituseta, kuid igal juhul ühe kuu jooksul pärast taotluse saamist. Seda ajavahemikku võib siiski pikendada kahe kuu võrra, võttes arvesse taotluste keerukust ja hulka, tingimusel, et isikule teatatakse tähtaja pikendamisest. Lisaks tuleb taotlusi käsitleda **tasuta**. Kui lükkate taotluse tagasi, siis tuleb Teil asjaomast isikut teavitada tagasilükkamise põhjustest ja sellest, et tal on õigus esitada kaebus andmekaitseasutusele.

Tõestage järgimist ja pidage arvestust!

Üks GDPRi aluspõhimõtteid on tagada, et ettevõtjad suudaksid tõestada selle nõuete järgimist. See tähendab, et peate suutma tõestada, et Teie ettevõte tegutseb kooskõlas GDPRi nõuetega ja täidab kõiki asjakohaseid kohustusi, eriti andmekaitseasutuse taotlusel või inspekteerimisel.

Selleks on üks võimalus pidada üksikasjalikku arvestust näiteks järgmise kohta:

- Teie ettevõttes andmetöötluses osalevate isikute nimed ja kontaktandmed;
- isikuandmete töötlemise põhjus(ed);
- isikuandeid andvate isikukategooriate kirjeldus;
- isikuandmeid saavate organisatsioonide kategooriad;
- isikuandmete edastamised teise riiki või teisele organisatsioonile;
- isikuandmete säilitamise aeg;
- isikuandmete töötlemisel kasutatud turvameetmete kirjeldus.

Peale selle tuleks Teie ettevõttes kehtestada kirjalik kord ja juhend, neid tuleks korrapäraselt värskendada ning teha need töötajatele teatavaks.

4.

KAS OLETE TÄITMISEKS VALMIS?

.GDPRi kohaselt on järgmine samm isikuandmete töötlemise alal Teie teha. Esiteks tuleks kaardistada oma praegune andmetöötlusega seotud tegevus ja hinnata oma ettevõttesiseseid protsesse. Eelkõige peate tegema järgmist:

- tegema kindlaks, mis andmeid Teie valduses on ning mis eesmärgil ja juriidilisel alusel Te neid säilitate;
- hindama kõiki sõlmitud lepinguid, eriti vastutavate ja volitatud töötlejate vahelisi lepinguid;
- kaaluma kõiki rahvusvahelise andmeedastuse jaoks kättesaadavaid kanaleid;
- vaatama üle oma ettevõtte üldise juhtimissüsteemi (st kasutatavad IT-süsteemid ja korralduslikud meetmed), sealhulgas tegema kindlaks, kas peate või tahate määrata andmekaitseametniku või mitte.

Selle protsessi käigus on tähtis tagada, et Teie ettevõtte tippjuhtkond osaleks nendes ülevaatamistes ja jagaks oma arvamusi, saaks korrapäraselt uut teavet andmekaitsepoliitika muudatuste kohta ning annaks sellega seoses nõu.

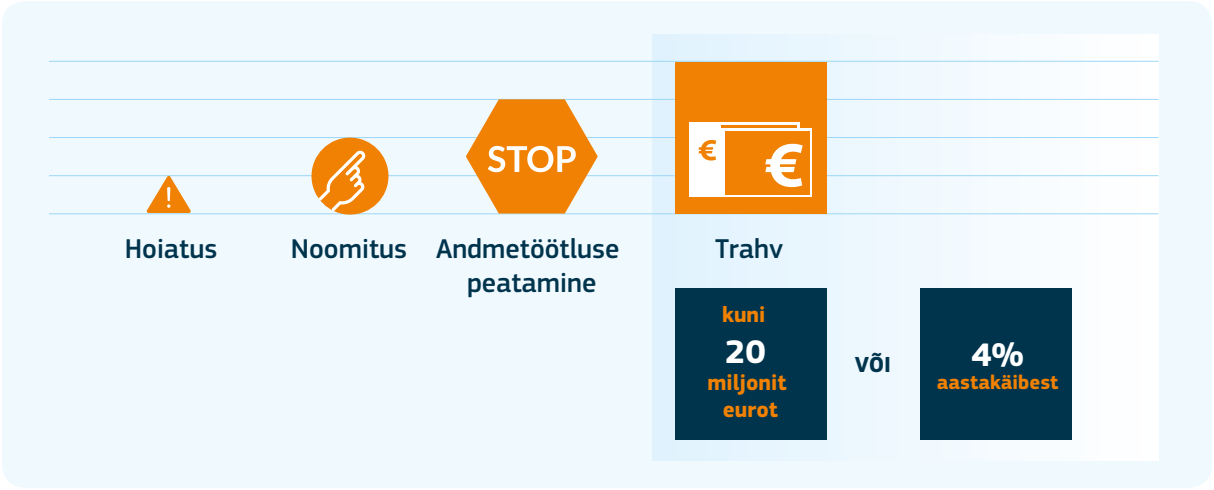
Kas töötlete andmeid mitmes riigis?

Piiriülese töötlemise korral võib pädevaks asutuseks olla teise riigi järelevalveasutus, mitte Teie riiklik andmekaitseasutus. Tavaliselt on selleks Teie ettevõtte ELis asuva põhitegevuskoha (töötlemise eesmärgi ja vahendite kohta otsuste tegemise koha) riiklik andmekaitseasutus.

Mittetäitmise riskid

GDPRi nõuete mittetäitmine võib tuua kaasa märkimisväärseid trahve: teatavate rikkumiste korral kuni 20 miljonit eurot või 4% Teie ettevõtte ülemaailmsest kogukäibest. Andmekaitseasutus võib määrata ka täiendavaid parandusmeetmeid, näiteks anda korralduse isikuandmete töötlemine lõpetada. Samuti peaksite mõtlema kahjule, mida mittetäitmine võiks Teie mainele põhjustada.

Selge, et GDPRi mittetäitmise kulud on palju suuremad kui mis tahes investeeringud selle nõuete täitmiseks.



Kas Teil on küsimusi? Muresid? Pöörduge riikliku andmekaitseasutuse poole.

Leidke veebi kaudu oma riigi andmekaitseasutus

http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

TÄHTIS TEAVE

Selles brošüüris olev teave ja nõuanded on ettenähtud selleks, et aidata ELi andmekaitse eeskirjadest paremini aru saada.

See on mõeldud üksnes nõustamisvahendiks, sest ainult isikuandmete kaitse üldmääruse tekstil on õiguslik jõud. Seetõttu saab ainult isikuandmete kaitse üldmäärus anda üksikisikutele õigusi ja kohustusi. Käesolevad nõuanded ei loo mingeid jõustatavaid õigusi ega ootusi.

ELi õigusaktide siduv tõlgendamine kuulub üksnes Euroopa Kohtu pädevusse. Käesolevates nõuannetes väljendatud seisukohad ei mõjuta seisukohta, mille komisjon võib Euroopa Kohtus võtta.

Euroopa Komisjon ega ükski tema nimel tegutsev isik ei vastuta käesolevas väljaandes esitatud teabe kasutamise eest.

Käesolev brošüür lähtub selle koostamise aja olukorrast ja seda tuleks pidada „arenevaks dokumendiks“, mida tuleb täiendada ja mille sisu võidakse ette teatamata muuta.

Võta ühendust ELiga

Isiklikult

Kõikjal Euroopa Liidus on sadu Europe Directi teabekeskusi. Teile lähima keskuse aadressi leiate: https://europa.eu/european-union/contact_et

Telefoni või e-postiga

Europe Direct on teenus, mis vastab Teie küsimustele Euroopa Liidu kohta. Teenusega saate ühendust võtta:
– helistades tasuta numbril: 00 800 6 7 8 9 10 11 (mõni operaator võib nende kõnede eest tasu võtta),
– helistades järgmisel tavanumbril: +32 22999696 või
– e-posti teel: https://europa.eu/european-union/contact_et

ELi käsitleva teabe leidmine

Veebis

Euroopa Liitu käsitlev teave on kõigis ELi ametlikes keeltes kättesaadav Euroopa veebisaidil: https://europa.eu/european-union/index_et

ELi väljaanded

Tasuta ja tasulisi ELi väljaandeid saab alla laadida või tellida EU Bookshopi kaudu: https://publications.europa.eu/bookshop
Suuremas koguses tasuta väljaannete saamiseks võtke ühendust talitusega Europe Direct või oma kohaliku teabekeskusega (vt https://europa.eu/european-union/contact_et).

ELi õigus ja seonduvad dokumendid

ELi käsitleva õigusteabe, sealhulgas alates 1952. aastast kõigi ELi õigusaktide konsulteerimiseks kõigis ametlikes keeleversioonides vt EUR-Lex: http://eur-lex.europa.eu

ELi avatud andmed

ELi avatud andmete portaal (http://data.europa.eu/euodp/et) võimaldab juurdepääsu ELi andmekogudele. Andmeid saab tasuta alla laadida ja taaskasutada nii ärilisel kui ka mitteärilisel eesmärgil.

DS-01-18-082-ET-C

Isikuandmete kaitse üldmäärus (inglise k *General Data Protection Regulation*, GDPR) reguleerib isikuandmete töötlemist ja haldamist ettevõtetes. Kui kogu Euroopas kehtib ühtne isikuandmete kaitse määrus, peab Teie ettevõte nüüd kogu ELis kaupu müües ja teenuseid osutades järgima peamiselt ühteainsat andmekaitseseadust.

Ettevõtjate jaoks õiguskeskkonda lihtsustades kujutab isikuandmete kaitse üldmäärus endast Teie ettevõtte jaoks uut võimalust parandada isikuandmete haldamist ning selle kaudu suurendada ka tarbijate usaldust Teie ettevõtte vastu.

Käesolevas brošüüris tuuakse esile kohustused, mida Teie ettevõte peab isikuandmete kaitse üldmääruse alusel täitma.

europa.eu/dataprotection/et

Väljaannete talitus

ISBN 978-92-79-79447-6