BALTIC RESTAURANTS ESTONIA AS PRIVAATSUSPOLIITIKA

Selles privaatsuspoliitikas („privaatsuspoliitika") kirjeldame, kuidas Baltic Restaurants Estonia AS („ettevõte") töötleb oma töötajate, klientide või ettevõttega muul moel koostööd tegevate inimeste isikuandmeid ning milliseid meetmeid me isikuandmete kaitsmiseks rakendame.

Isikuandmeid töödeldakse isikuandmete kaitse üldmääruse (määrus (EL) 2016/679) ning muude siseriiklike ja Euroopa privaatsusseaduste ning regulatsioonide (ühiselt „andmekaitseseadus") kohaselt.

1. ULATUS

Käesolev privaatsuspoliitika kohaldub kõigile isikuandmetele, mida vastutava töötlejana töötleme.

Ettevõte töötleb näiteks töötajate, ajutiste töötajate, füüsilisest isikust ettevõtjate, töö- ja ametikohale kandideerijate, tarnijate kontaktisikute, klientide ja külaliste ja muude koostööpartnerite isikuandmeid.

2. EESMÄRK

Selle privaatsuspoliitika eesmärk on selgitada, milliseid isikuandmeid me töötleme ning kuidas ja miks seda teeme. Lisaks kirjeldab see privaatsuspoliitika meie kohustusi ja vastutust andmete kaitsmisel.

See privaatsuspoliitika ei kajasta meie andmekaitsealaseid tegevusi ammendavalt, erinevates valdkondades, nagu nt turvalisus, sätestatakse täpsemad reeglid ja juhendid, millest mõistlikus ulatuses ettevõtte siseselt ka teavitame.

MÕISTED

Selles privaatsuspoliitikas kasutatakse mõisteid järgmises tähenduses:

EMP – Euroopa majanduspiirkond

GDPR – on ELi isikuandmete kaitse üldmäärus (general data protection regulation, (EU) 2016/679), mille rakendamine algas 25. mail 2018.a.

Isikuandmed – on igasugused andmed ja teave, mis on seotud füüsilise isiku ehk inimesega ja mis võimaldavad selle inimese isikut tuvastada. Isik on tuvastatav, kui tema isikut saab andmete põhjal ebaproportsionaalse pingutuseta mõistlikus ulatuses tuvastada. Tuvastamise aluseks võib olla näiteks nimi, isikukood, asukohateave, võrguidentifikaator või füüsiline, füsioloogiline, geneetiline, vaimne, majanduslik, kultuuriline või sotsiaalne tunnus või selliste tunnuste kombinatsioon.

Isikuandmete eriliigid – on isikuandmed, millest ilmneb inimese rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, aga ka geneetilised andmed, inimese kordumatuks tuvastamiseks kasutatavad biomeetrilised andmed, terviseandmed või andmeid füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta.

Isikuandmetega seotud rikkumine – on turberikkumine, mille tagajärg on edastatavate, talletatavate või muul viisil töödeldavate isikuandmete tahtmatu või ebaseaduslik hävimine, kaotsiminek, muutmine, lubamatu avaldamine või lubamatu juurdepääs neile andmetele.

Klient – on füüsiline isik, kellele ettevõte seoses oma majandustegevusega osutab teenuseid ja/või pakub kaupu.

Kolmas isik – on füüsiline või juriidiline isik, avaliku sektori asutus, amet või organ, välja arvatud andmesubjekt, vastutav töötleja või volitatud töötleja ja isikud, kes võivad isikuandmeid töödelda vastutava töötleja või volitatud töötleja otseses alluvuses.

Koostööpartner – füüsiline isik, kes on ettevõtte tarnija või muu juriidilisest isikust koostööpartneri töötaja/esindaja/kontaktisik.

Profiilianalüüs – on igasugune isikuandmete automatiseeritud töötlemine, mis hõlmab isikuandmete kasutamist füüsilise isikuga seotud teatavate isiklike aspektide hindamiseks, eelkõige selliste aspektide analüüsimiseks või prognoosimiseks, mis on seotud selle füüsilise isiku töötulemuste, majandusliku olukorra, tervise, isiklike eelistuste, huvide, usaldusväärsuse, käitumise, asukoha või liikumisega.

Töötlemine – on isikuandmetega tehtav toiming või toimingute kogum, nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine. Töötlemine võib toimuda käsitsi või automatiseeritud süsteeme, näiteks IT-süsteeme kasutades.

Töövõtja – on füüsiline isik (st mitte ettevõte), kellega ettevõte on sõlminud töövõtulepingu (teenuse osutamise leping), siia kuuluvad ka ettevõtte juhtorganite liikmed.

Vastutav töötleja – on isik, kes otsustab, miks ja kuidas (st mis eesmärkidel ja viisidel) isikuandmeid töödeldakse. Vastutava töötleja kindlakstegemisel võib olla abi järgmistele küsimustele vastamisest.

- Kes otsustab, milliseid isikuandmeid säilitatakse?
- Kes otsustab, mis eesmärkidel isikuandmeid kasutatakse?
- Kes otsustab, mis viisil isikuandmeid töödeldakse?

Kui isik otsustab ise tema valduses olevate isikuandmete töötlemise üle ja on nende eest vastutav, siis on ta vastutav töötleja.

Volitatud töötleja – on isik, kes töötleb isikuandmeid vastutava töötleja nimel. Kui isikuandmed on isiku valduses või ta töötleb neid, kuid tal ei ole voli nende töötlemise üle otsustamiseks, st ta töötleb neid vastutava töötleja juhiseid järgides, siis on see isik volitatud töötleja. Volitatud töötlejaks võib olla nt teenuse osutaja (näiteks palgaarvestusteenuse osutaja).

1. ISIKUANDMETE KATEGOORIAD

1.1 Töötajad ja töövõtjad

Ettevõte töötleb oma töötajate, töö- ja ametikohtadele (nt juhatuse liikmed) kandideerijate ja töövõtjate kohta, samuti endiste töötajate ja endiste töövõtjate kohta.

Need isikuandmed hõlmavad järgmist:

- isiklikud andmed, nagu nimi, sünniaeg, pangakonto andmed, lähisugulased, sotsiaalmeedia konto andmed, viisa-/passi-/ID kaardi andmed või vastava dokumendi koopia;
- kontaktandmed, nagu aadress ja telefoninumber, e-posti aadress;
- personalifaili andmed, muu hulgas: töösuhte tingimused, koolitusandmed, töötulemuste hindamised/hinnangud, edutamised, isiklikud arenguplaanid, käitumis- ja distsiplinaarandmed, töö asukoht, palgaandmed, pangakonto andmed ning maksukohustuslase number ja isikukood;
- töösuhete ajaloo / kandideerimise andmed, näiteks hariduse ja varasemate töösuhete ajalugu;
- pereliikmete andmed, näiteks laste sünniajad ja nimed (need on asjakohased näiteks juhul, kui inimene taotleb vanemapuhkust);
- ametiühingu liikmesust puudutavad andmed;
- tööalase sooritusega seotud andmed, näiteks töötajate iga-aastane palga ülevaatamine, psühhomeetrilised testid jne.

- Isikuandmete eriliigid: meditsiinilised andmed, näiteks arstitõendid ja haiguslehed;

Ülaltoodud loetelu ei ole ammendav, kuid hõlmab kõige sagedamini kogutavaid, kasutatavaid ja muul viisil töödeldavaid isikuandmeid.

1.3 Koostööpartnerid

Ettevõte töötleb oma koostööpartnerite isikuandmeid. Selliseid isikuandmed võivad hõlmata järgmist:

- isiklikud andmed, näiteks nimi, ametinimetus, ametikoht, tööalased identifitseerimisnumbrid, osakond, äriüksus (sh koolituse/kontrollimise jaoks kogutavad kontaktandmed);
- kontaktandmed, näiteks meiliaadress, telefoninumbrid ja töö asukoht;
- maksuandmed, näiteks käibemaksu-/maksukohustuslase numbrid.

2. ANDMETE TÖÖTLEMISE EESMÄRGID

Ettevõte töötleb isikuandmeid nendel eesmärkidel, milleks isikuandmed on kogutud.

Töötajate isikuandmeid töötleme näiteks järgmistel eesmärkidel:

- töölepinguseaduses ettevõttele sätestatud tööandja kohustuste täitmine;
- palga ja hüvitiste haldamine;
- personalitegevuste, soorituse ja talendi juhtimine;
- siseauditid (töökeskkond ja tööohutus);

Klientide ja koostööpartnerite isikuandmeid töötleme näiteks järgmistel põhjustel:

- kliendi/koostööpartneriga sõlmitud lepingu ettevalmistamine ja selle täitmine;
- turundus ja avalikud suhted;
- ettevõtte toodete ja teenuste täiustamine;
- uurimistöö ja statistiline analüüs;
- ettevõtte äristrateegia kujundamine;
- ettevõtte või meie klientide ja töötajate suhtes ebaseadusliku ja/või kuritegeliku käitumise vältimine ja tuvastamine.

Aeg-ajalt võime töödelda isikuandmeid ka muudel põhjustel. Ettevõte püüab tagada inimeste teavitamise nende isikuandmete töötlemise eesmärkidest isikuandmete saamise ajal. Kui see pole võimalik või mõistlik, siis üritame inimesi teavitada esimesel võimalusel pärast isikuandmete saamist või muul viisil töötlemist.

3. PROFIILIANALÜÜS

Ettevõte teeb erinevate inimeste (nt töötajate, töövõtjate ja töö- või ametikohale kandideerijate) osas profiilianalüüsi.

Ettevõte töötleb selliseid andmeid, kui: a) see on seadustega sõnaselgelt lubatud; b) see on vajalik lepingu sõlmimiseks või täitmiseks või c) inimene on andnud selleks nõuetekohase nõusoleku.

Juhul, kui teeme automatiseeritud otsuseid, sealhulgas profiilianalüüsi, siis teavitame inimesi kasutatavast loogikast ja sellest, milline on sellise töötlemise tähtsus ja prognoositavad tagajärjed andmesubjekti jaoks.

4. ANDMESUBJEKTI ÕIGUSED

Inimestel on andmekaitseseaduse alusel oma isikuandmetega seonduvalt teatud õigused.

4.1. Õigus andmetega tutvuda – inimesel on õigus teada, milliseid andmeid teie kohta säilitatakse ja kuidas neid töödeldakse.

4.2. Õigus andmete parandamisele – inimesel on õigus nõuda oma isikuandmete parandamist, juhul kui need on ebaõiged.

4.3. Õigus andmete kustutamisele („õigus olla unustatud“) – inimesel on teatud juhtudel õigus nõuda, et me tema isikuandmed kustutaksime (nt kui meil ei ole neid enam vaja, jne).

4.4. Õigus töötlemise piiramisele – inimesel on teatud juhtudel õigus keelata või piirata oma isikuandmete töötlemist teatud ajaks (nt kui ta on esitanud vastuväite andmetöötluse osas).

4.5. Õigus esitada vastuväiteid – konkreetsest olukorrast lähtuvalt on inimesel õigus esitada oma isikuandmete töötlemise osas vastuväiteid kui inimese andmete töötlemine toimub meie õigustatud huvist lähtudes või avalikust huvist lähtudes. Otseturunduse eesmärgil isikuandmete töötlemisele võib esitada vastuväiteid igal ajal.

4.6 Õigus andmete ülekandmisele – Juhul, kui isikuandmete töötlemine põhineb inimese nõusolekul või ettevõttega sõlmitud lepingul ja andmeid töödeldakse automatiseeritult, siis on inimesel õigus saada teda puudutavaid isikuandmeid, mida ta on vastutavale töötlejale esitanud, struktureeritud, üldkasutatavas vormingus ning masinloetaval kujul ning õigus edastada need andmed teisele vastutavale töötlejale. Samuti on tal õigus nõuda, et ettevõte edastaks andmed otse teisele vastutavale töötlejale, kui see on tehniliselt teostatav.

4.7. Automaatse otsuste tegemine (sh profiilianalüüs) – juhul, kui oleme teavitanud, et teostame automatiseeritud töötlusel põhinevat otsustamist (sh profiilianalüüsi), mis toob kaasa teid puudutavaid õiguslikke tagajärgi või avaldab teile märkimisväärset mõju, siis võib inimene nõuda, et otsust ei tehtaks üksnes automatiseeritud töötluse alusel.

Andmesubjekti õiguste ja taotluste protseduuris on selgitatud, kuidas eespool nimetatud õigustega seotud taotlusi saab esitada ja kuidas ettevõte selliseid taotlusi haldab.

4.8 Lisaks õigusele salvestistega tutvuda on isikul õigus kasutada ka kõiki muid andmesubjekti õigusi, mis on sätestatud Euroopa Parlamendi ja Nõukogu määruses (EL) 2016/679. Andmesubjekti õigused on kirjeldatud ka Baltic Restaurants Estonia AS privaatsuspoliitika punktis 4 („Andmesubjekti õigused“). Ja andmete kogumise aluseks olevate õiguslike analüüsidega Oma õiguste teostamiseks palume ühendust võtta personali äritegevuse juhiga telefonil +372 53855373.

4.9 Kõikidel andmesubjektidel on õigus pöörduda kaebusega riikliku andmekaitse järelevalve teostaja poole, kui andmesubjekt leiab, et temaga seotud isikuandmete töötlemine ei vasta andmekaitseseaduste ja üldiste andmekaitsereeglite sätetele. Eestis on riiklikuks järelevalve teostajaks Andmekaitse Inspektsioon.

5. TURVE

5.1 Turbemeetmed

Ettevõttes on kehtestatud füüsilised, tehnilised ja organisatsioonilised meetmed isikuandmete kaitsmiseks ebaseadusliku või omavolilise hävitamise, kaotsimineku, muutmise, avaldamise, omandamise või neile lubamatu juurdepääsu eest.

Ettevõtte kasutab näiteks järgmisi füüsilisi andmeturbe meetmeid:

- isikuandmeid sisaldavaid paberkandjal dokumente hoitakse lukustatud ruumides ja kappides, millele on ligipääs vaid teatud töötajatel oma tööülesannete täitmiseks;
- andmete töötlemise ruumid ja IT-süsteemid on piisavalt kaitstud tule, ülekuumenemise, vee, voolukõikumiste ja voolukatkestuste eest.

Tehniliste turbemeetmetena on ettevõttes kasutusel näiteks:

- videovalve;

- kõik tööarvutid on töötaja lahkumisel parooliga ekraanisäästjaga kaitstud;
- on tagatud, et IT-süsteem ei võimalda uusi sisenemiskatseid ja lukustab kasutajatunnuse, kui ebaõnnestunud sisenemiskatsete arv ületab teatud piiri;
- on tagatud, et eriti ohustatud süsteemid (nt sülearvutid, nutitelefonid) on piisavalt hästi kaitstud (kasutades näiteks krüpteerimist või muid viise).

Organisatsiooniliste turbemeetmetena kasutame:

- juurdepääsud olulistele IT süsteemidele ja ruumidele on reguleeritud;
- kõigile IT süsteemide kasutajatele on määratud rollid ja profiilid;
- on kindlaks määratud, millistele andmetele millised kasutajad ligi pääseda tohivad ning ligipääsuõigused vastavad töötaja tööülesannetest tulenevatele vajadustele;
- on tagatud, et ligipääsuõigused tühistatakse töötaja lahkumisel ettevõttest;
- on tagatud, et avalikult kasutatavatest ruumidest ei pääse ilma volituseta ruumidesse, mida kasutatakse isikuandmete töötlemiseks;
- ettevõtte külastajate (st mitte avalikult kasutatavate ruumide külastajate) tarvis on koostatud külastuskord ning külastajate andmed, saabumis- ja lahkumisajad registreeritakse saabumisel ja lahkumisel;
- ruumid, kus asuvad IT-süsteemile ligipääsu võimaldavad arvutid ja ruumid, kus hoitakse isikuandmeid sisaldavaid dokumente, on kontrolli/valve all ka peale tööaja lõppu.

6. ISIKUANDMETE AVALDAMINE

Ettevõte võib aeg-ajalt isikuandmeid kolmandatele isikutele avaldada või neil ettevõttes töödeldavatele isikuandmetele juurde pääseda (näiteks kui õiguskaitseasutus või Andmekaitse Inspektsioon esitab kehtiva nõude isikuandmetele juurdepääsemiseks).

Ettevõte võib jagada isikuandmeid ka: a) teise ettevõttega samasse kontserni kuuluva isikuga (nt Lätis asuv BRL); b) valitud muude osapooltega, sh äripartnerid, tarnijad ja töövõtjad; c) muude osapooltega, kui müüme või ostame teisi ettevõtteid või varasid (st tehingute tegemisel), või d) kui ettevõttel on seaduslik kohustus isikuandmeid avaldada (see hõlmab teabevahetust teiste ettevõtete ja organisatsioonidega pettuste vältimiseks).

Kui ettevõte sõlmib muude osapooltega lepinguid isikuandmete töötlemiseks ettevõtte nimel, tagab ta sobivate lepinguliste kaitsemeetmete olemasolu isikuandmete kaitsmiseks, kasutades muuhulgas andmekaitse standardklausleid, mis on välja töötatud ettevõtte nimel andmeid töötlevate isikutega sõlmitavatesse lepingutesse lisamiseks.

Ettevõte avaldab isikuandmeid või annab neile juurdepääsu järgmiste isikute kategooriatele allpool selgitatud eesmärkidel:

- sideteenuste osutajad – töötajate kõne- ja andmesideteenuste korraldamiseks;
- palgaarvestuse teenuse osutajad – töötajate palgaarvestuse pidamiseks;
- töötervishoiuteenuse osutajad – töötajate töötervishoiu korraldamiseks;
- värbamisagentuurid – uute töötajate/töövõtjate leidmiseks;
- turundusettevõtted – ettevõtte poolt nimetatud klientidele otseturunduse tegemiseks;
- kindlustusvahendajad ja kindlustusandjad – ettevõtte töötajate reisi-, õnnetusjuhtumi-, vms sellise kindlustuse tegemiseks.

7. ANDMETE SÄILITAMINE

Ettevõte säilitab isikuandmeid ainult seni, kuni selliste isikuandmete säilitamist peetakse vajalikuks eesmärkidel, milleks neid isikuandmeid koguti. Isikuandmeid säilitatakse asjakohaste seaduste ja ettevõtte põhimõtete kohaselt.

Ettevõte lähtub isikuandmete säilitamisel järgmistest kriteeriumidest:

- kui kaua kui on vaja isikuandmeid säilitada selleks, et pakkuda oma teenuseid
- kui ettevõttel on seadusest tulenev, lepinguline või muu sarnane kohustus isiku andmete säilitamiseks, siis seni kuni on vajalik sellise kohustuse täitmiseks
- peale lepingulise suhte lõppemist säilitame teatud andmeid nii kaua, kui kaua on isikul (andmesubjektil) või ettevõttel endal õigus esitada lepingu alusel nõudeid teise poole vastu.

Mõned näited:

- Töölepingu kirjalikke dokumente säilitame töölepingu seaduse nõuete kohaselt 10 aastat töölepingu lõppemisest.
- Tööohutusalaseid dokumente säilitame 55 aastat.

8. ANDMEEDASTUS VÄLJASPOOLE EMPd

Aeg-ajalt võib ettevõttel olla vaja edastada isikuandmeid väljaspool EMPd. Selline edastus toimub kehtiva andmekaitseseaduse kohaselt[1]. Ettevõte võtab tarvitusele mõistlikke abinõusid tagamaks, et isikuandmeid koheldakse EMPst väljapoole edastamisel turvaliselt ja selle privaatsuspoliitika kohaselt.

Ettevõte edastab isikuandmeid järgmistesse asukohtadesse väljaspool EMPd allpool nimetatud eesmärkidel, kasutades järgmisi meetmeid isikuandmete kaitseks:

- Seaduslikku õigust omavad asutused
- Kohtuotsuse alusel

9. VASTUTUSALAD

Ettevõte vastutab isikuandmete töötlemise eest. Üldine vastutus selle privaatsuspoliitika järgimise eest ettevõttes lasub ettevõtte juhtkonnal, kes määrab peamise kontakti seoses a) ettevõtte töötajate ja töövõtjate isikuandmete töötlemise; b) koostööpartnerite isikuandmete töötlemise ja c) ettevõttes töödeldavate isikuandmete turvalisusega.

Kõigil ettevõtte töötajatel, kes puutuvad kokku isikuandmete töötlemisega on kohustus järgida kõige ajakohasemat avaldatud versiooni sellest privaatsuspoliitikast. Kõikide küsimuste puhul tuleb ühendust võtta personali äritegevuse juhiga.

10. SEOTUD REEGLID JA PROTSEDUURID

Seda privaatsuspoliitikat tuleb lugeda koos järgmiste reeglite ja protseduuridega:

- Töökorralduse reeglid

[1] GDPR artiklid 45-49 sätestavad millal ja mis tingimustel on andmete edastamine lubatud. GDPRi artikkel 45 kohaselt võib isikuandmeid EList väljapoole edastada siis, kui Euroopa komisjon on teinud otsuse, et selline kolmas riik, territoorium või rahvusvaheline organisatsioon tagab isikuandmete kaitse piisava taseme. Selliseks edastamiseks ei ole vaja eriluba. Sellised riigid, territooriumid või rahvusvahelised organisatsioonid avaldatakse Euroopa Liidu Teatajas ja komisjoni veebilehel.

11. TURVAKAAMERATE KASUTAMISE ÕIGUSTATUD HUVI KLIENITSOONIS

Baltic Restaurants Estonia AS kasutab turvakaameraid isikute (so klientide ja töötajate) kaitsmiseks, ohutuse tagamiseks ja sisekorraeeskirjade järgimise tuvastamiseks. Isikuandmete vastutav töötleja on Baltic Restaurants Estonia AS.

Turvakaamerad on paigutatud selliselt, et jälgimisalasse jäävad müügilett ja kassa. Sellest tulenevalt jäävad jälgimisalasse ning videosalvestistele ka nimetatud alades tegutsevad ettevõtte töötajad, kliendid ja muud külastajad, kes on seotud kuidagiviisi ettevõtte müügiala korrasoleku või tehnilise toega (näiteks: tehnikud).

Videokaamerate kasutamise põhitingimused:

Kaamerate kasutamise õiguslik alus – õigustatud huvi.

Jälgimissüsteemi lühike kirjeldus – digitaalne ilma helisalvestamise võimeta.

Kellele salvestis võidakse edastada – PPA-le, AKI-le ja teistele seadusest tulenevatele asutustele ja isikutele.

Juurdepääs jälgimissüsteemile ja salvestistele on ettevõtte kontrolleril, IT-administraatoril ja piirkonna teenindusjuhil. Salvestised paiknevad koostööpartneri serveris. Vastavalt koostööpartneriga sõlmitud kokkuleppele ei ole koostööpartneril ligipääsu salvestistele vaid koostööpartner haldab salvestiste logi. Salvestiste vaatamine toimub vastavalt vajadusele (teenindusprotsessi jätkusuutlikkuse kontroll, töötaja pöördumine, seoses töökeskkonna probleemiga, kliendipöördumine või õiguskaitseorganite pöördumine).

Salvestise säilitamine – salvestisi säilitatakse 30 kalendripäeva, misjärel hakkab videosüsteem automaatselt üle salvestama. Turvaintsidendi korral säilitatakse intsidendiga seotud salvestist kuni intsidendi lahendamiseni.

Jälgimise aeg – ööpäevaringselt.

Jälgimise liik – reaalajas salvestamise ja järele vaatamisega.

ÕIGUSTATUD HUVI TUVASTAMINE

Baltic Restaurants Estonia AS (edaspidi “vastutav töötleja”) on paigaldanud müügileti, kassa juurde kaamerad, mille vaatevälja võivad jääda kliendid, ettevõtte töötajad või ettevõtte lepingulised koostööpartnerid. **Isikuandmete töötlemisel on ettevõttel 3 eesmärki**

- Ettevõte peab tagama ohutu töökeskkonna oma personalile ja kokkulepitud töökorralduslike reeglite täitmise. Teenuse jätkusuutliku pakkumise tagamisel on ettevõttel oluline järgida, et töötajad täidavad kokku lepitud töökorralduslikke reegleid ja sealhulgas oleks tagatud ka ohutu töökeskkond.
- Teenuse sujuv pakkumine kliendile. Samuti on meile oluline, et tagatud on ka klientide turvalisus.
- Ettevõtte vara kaitsmine, mille kadumine või hävimine tooks ettevõttele majanduslikku kahju. Isikuandmete töötlemise eesmärk on ennetada, ohjata ja märgata süütegusid seoses omandi ja vara kaitsega. Ettevõte soovib tagada, et müügileti taha ei siseneks isikut, kellel selleks õigust ei ole (nad ei ole ettevõtte töötajad ega lepingulised partnerid).

Juhindume GDPRi artiklis nr 47, kus on mainitud, et pettuste vältimiseks rangelt vajaliku isikuandmete töötlemise puhul võib tugineda õigustatud huvile. Antud juhul ei ole tegemist otseselt pettuste ärahoidmisega, vaid eesmärgiks on nii ettevõtte töötajate, klientide ohutuse tagamine kui ka ettevõtte vara kaitse tagamine, samuti töökorralduslike reeglite rikkumiste tuvastamine. Need eesmärgid on sarnased pettuste ärahoidmise eesmärgiga.

Isikuandmete töötlemine on vastutava töötleja jaoks oluline, sest ettevõtte jaoks on oluline nii töötajate kui ka klientide turvalisuse ja teenusega rahulolu tagamine.

Ettevõtte vara kahjustamise ärahoidmiseks või peatamiseks, samuti ettevõtte töötajaid ning kliente ohustava tegevuse ärahoidmiseks või peatamiseks ei ole tõhusamaid viise. Videovalve võimaldab

vaadelda reaalajas kui ka toimunud sündmusi tagant järele ja tuvastada rikkumine. Ning hiljem leida lahendusi tekkinud probleemidele. Kaamerate kasutamine on levinud viis toimunud sündmuste hilisemaks tuvastamiseks ja tõendamiseks.

Vastutav töötleja on taganud teavitussiltide olemasolu, et andmesubjekt saaks aru, et teda jälgitakse kõnealuses piirkonnas kaameraga. Siiski on risk, et salvestise peale võib tundlikku informatsiooni jääda. On võimalik, et andmesubjekt ei pane tähele silti, mis kaamera olemasolust teavitab. Samas on see risk, mida ei saagi täielikult kõrvaldada. Vastutav töötleja on teinud kõik endast oleneva, et andmesubjekte kaameraga jälgimisest teavitada.

Ettevõte on analüüsinud olukorda, et kui kõnealust isikuandmete töötlemist ei toimuks, siis on risk, et vastutav töötleja ei suuda ära hoida enda vara kahjustamist või ohu tekkimist enda töötajatele ja klientidele. Samuti on sellisel juhul risk, et vastutav töötleja ei avasta piisavalt kiiresti töökorralduslike reeglite rikkumisi, mis võib omakorda tekitada ohu töötajatele või klientidele.

Turvaline keskkond ei ole ainult vastutava töötleja huvides vaid ka ettevõtte personali ja teenust kasutava kliendi huvides.

11.1 Teabe töötlemine

Isikuandmeid kogutakse otse andmesubjektilt (vastutav töötleja on see isik, kes andmesubjekti kaameraga jälgib).

Töödeldakse teavet, mis jääb kaamera vaatevälja. Kuivõrd tegemist on isikute reaalajas kaamerate jälgimisega, eksisteerib võimalus, et kaamerasalvestisele jääb tundlikku teavet. Seda riski on püütud maandada sellega, et enne kaameraga jälgitavale alale sisenemist näeb isik teavitust kaamera kasutamise kohta. Kaameratega jälgitakse ainult müügiletti ja kassat.

Salvestistele ligipääs - salvestised asuvad virtuaalserveris, kuhu on juurepääs vaid ettevõtte kontrolleril, IT administraatoril ja piirkonna teenindusjuhil personaalsete kasutajatunnuste ning paroolidega.

Kogutud andmetega tutvumine – isiku kohta kogutud andmetega tutvumiseks palume esitada taotlus kirjalikult e-postile office@balticrest.com . Andmetega tutvumisel tuleb arvestada sellega, et säilitame salvestisi 30 päeva, samuti sellega, et teiste salvestisele jäädvustatud isikute õiguste ja huvide kaitsmiseks peame muutma nad tuvastamatuks, mistõttu ei saa me tutvumist võimaldada koheselt. Kui taotlus esitatakse ajal, mil andmed on alles, siis need edastatakse peale taotluse kättesaamist 14 päeva jooksul.

Lisaks õigusele salvestistega tutvuda on isikul õigus kasutada ka kõiki muid andmesubjekti õigusi, mis on sätestatud Euroopa Parlamendi ja Nõukogu määruses (EL) 2016/679. Andmesubjekti õigused on kirjeldatud privaatsuspoliitika punktis 4 („Andmesubjekti õigused“). Ja andmete kogumise aluseks olevate õigusliku analüüsiga.

Oma õiguste teostamiseks palume ühendust võtta ettevõttega e-posti teel office@balticrest.com või telefonil +372 53855373.

Vastutav töötleja on andmesubjekti põhiõiguste- ja vabaduste kaitseks rakendanud järgnevad meetmed:

1) andmesubjekti on teavitatud videovalve tingimustest kodulehel privaatsustingimustes;

2) vastutav töötleja on paigutanud kaameraga jälgimisele osutavad teavitussildid;

3) vastutav töötleja on hoolikalt läbi mõelnud, kuidas käib andmesubjekti päringutele vastamine, sh olukorras, kus andmesubjekt näiteks soovib tutvuda salvestisega, millele ta on jäädvustatud või kui andmesubjekt taotleb salvestise kustutamist;

4) vastutav töötleja on kehtestanud tähtajad videosalvestiste säilitamisele. Salvestisi säilitatakse 30 kalendripäeva. Pärast tähtaja möödumist hakkab videosüsteem automaatselt üle salvestama. Turvaintsidendi korral säilitatakse intsidendiga seotud salvestist kuni intsidendi lahendamiseni;

5) vastutav töötleja on kehtestanud juurdepääsu piirangud – salvestised asuvad virtuaalserveris, kuhu on juurepääs vaid ettevõtte volitatud isikutele ja paroolidega.

11.2 Järeldus

Arvestades ülaltoodut, tuleb järeldada, et kaamerate kasutamine müügileti ja kassa kohal, tuvastamaks võimalikke ohte turvalisusele ja tuvastamaks töökorralduslike reeglite rikkumisi, on üldmääruse artikkel 6 lg 1 punkti f alusel võimalik. Kuigi kaamerate kasutamise puhul on tegemist riivava isikuandmete töötlemise toiminguga, rakendab vastutav töötleja antud juhul meetmeid, mis tagavad töötlemise läbipaistvuse andmesubjekti jaoks ning andmesubjekti põhiõiguste ja -vabaduste kaitse.

Analüüsi lõppjäreldus: Vastutav töötleja saab kasutada kaameraid turvalisuse tagamise eesmärgil, tuginedes isikuandmete töötlemise õigusliku alusena õigustatud huvile (üldmääruse art 6 lg 1 punkt f).

Allkirjastaja: Aaro Lode

Ametikoht: Tegevjuht

Kuupäev: 07.03.2022

Kaalumisotsuse ülevaatamise kuupäev: 22.02.2022