Järeldused Balti riikide järelevalveasutuste ühiskontrolli kohta, mis käsitleb isikuandmete töötlemise nõuetekohasust sõidukite lühiajalise rentimise valdkonnas

I. ÜLDINE TEAVE

Balti riikide järelevalveasutused (Leedu Andmekaitse Inspektsioon, Läti Andmekaitse Inspektsioon, Eesti Andmekaitse Inspektsioon, edaspidi järelevalveasutused või -asutused) nõustusid tegema ennetavat kontrolli isikuandmete töötlemise nõuetekohasuse üle sõidukite lühiajalise rentimise valdkonnas.

Järelevalveasutused viisid läbi sõidukite lühiajalise rentimise teenuste valdkonnas ennetava kontrolli, et selgitada välja, kas Eestis, Lätis ja Leedus asutatud ja tegutsevad sõidukite lühiajalise rentimise teenuse osutajad, kes osutavad Balti riikides füüsilistele isikutele sõidukite lühiajalise rentimise teenuseid, järgivad Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta) sätteid, millega tunnistatakse kehtetuks direktiivi 95/46 EÜ (isikuandmete kaitse üldmäärus) sätted.

Koordineeritud järelevalvemeetmete rakendamine tuleneb järelevalveasutuste 2021. aasta kohtumisest, mille käigus leppisid järelevalveasutused kokku, et 2022.–2023. aastal korraldatakse Eestis, Lätis ja Leedus valdkondlik järelevalve eesmärgiga töötada välja soovitused isikuandmete töötlemise ja kaitse protsesside parandamiseks eelnevalt kokku lepitud sektoris.

Ametiasutused leppisid kokku kontrolliks valitud teenuseosutajate kriteeriumides:

- ✓ isikud, kes pakuvad sõidukite, sealhulgas elektritõukerataste lühiajalist rentimist (autojagamist);
- ✓ Peamine teenuse saaja on füüsiline isik;
- ✓ Tegevuskoht – Balti riigid.

II. Kontrolli ulatus

Kõik järelevalveasutused võtavad arvesse vähemalt mõnda allpool nimetatud kriteeriumi, säilitades samal ajal iga järelevalveasutuse vastutuse võtta sihtrühma valimisel arvesse muid aspekte, säilitades peamise kontrolliraamistiku (isikuandmete töötlemine, sõidukite lühiajalise rentimise teenuste osutamine füüsilistele isikutele, isikuandmete kaitse üldmääruse (IKÜM) järgimine):

- ✓ Ettevõtted, kes osutavad teenuseid kõigis Balti riikides ja sellised ettevõtted, kes osutavad teenuseid vähemalt kahes Balti riigis.
- ✓ ettevõtted, mille vastutav töötleja või kaasvastutav töötleja (IKÜM artikli 4 punktides 7 ja 8 määratletud isikuandmete kaitse eest vastutavad isikud) asub ühes Balti riikidest (konkreetsete ettevõtete inspekteerimise algatab riik, kus asub peamine tegevuskoht);
- ✓ ettevõtted, kelle tegevuse kohta esitatakse (võrreldes teiste samal turul tegutsevate ettevõtetega) kõige rohkem kaebusi/taotlusi;
- ✓ ettevõtted, mis hõivavad suurema osa sõidukite renditeenuste turust;
- ✓ Tarbijate poolt (osaliselt) finantseeritavad ettevõtted (Tuul Mobility OÜ on emiteerinud võlakirju);
- ✓ Ettevõtted, mis on tuntud oma laiahaardelise tarbijale suunatud reklaami kasutamise poolest.

Nimetatud kriteeriume arvestades valisid järelevalveasutused välja kaheksa ettevõtet, kes osutavad Balti riikide territooriumil sõidukite lühiajalise rentimise teenuseid (edaspidi ettevõtted):

1. Ltd. TRANSPORT (SIXT);
2. Ltd. SLYFOX (CARGURU);
3. Ltd. RIDE;
4. SIA "ETERNA ELECT" (Skok);
5. UAB „Peamine liising“ (CityBee).
6. Bolt Operations OÜ;
7. ELMO Rent AS (jälgitavad teenused on aruande valmimise ajaks lõpetatud);
8. Tuul Mobility OÜ.

Kontrolli käigus hinnati, kas isikuandmed, mida ettevõtted sõidukirenditeenuse osutamiseks töötlevad:

- ✓ on piisavad (IKÜM artikli 5 lõike 1 punkt c);

- ✓ töödeldakse vastavalt eesmärgile (IKÜM artikli 5 lõike 1 punkt b);
- ✓ järgivad säilitamise piiramise põhimõtet (IKÜM artikli 5 lõike 1 punkt e);
- ✓ omavad isikuandmete töötlemiseks asjakohast õiguslikku alust (IKÜM artikkel 6).

Tehes järelevalveasutuste päritoluriikides koordineeritud järelevalvet, on järelevalveasutused jõudnud suhteliselt sarnastele järeldustele seoses ebajärjepidevusega ettevõtete isikuandmete töötlemisel sõidukite lühiajalise rentimise valdkonnas, mis on esitatud allpool.

III. INSPEKTSIOONI JÄRELDUSED

1. Sobiva õigusliku aluse kindlaksmääramine.

Üks olulisemaid ebakõlasid, mis tuvastati sõidukite renditeenuse osutajate isikuandmete töötlemisel, on õigusliku aluse sobimatu valik või suutmatus tehtud valikuid piisavalt põhjendada. Mõnikord erinesid privaatsuspoliitikas (andmetöötluseeskirjad) täpsustatud töötlemise õiguslik alus ja töödeldavate isikuandmete hulk sellest, mida ettevõtted esitasid oma vastustes järelevalveasutustele. Samuti on olnud juhtumeid, kus kõigile töötlemistoimingutele, sealhulgas töötlemistoimingutele, mille puhul seda õiguslikku alust ei kohaldata, on määratud üks õiguslik alus.

Isikuandmete töötlemise õiguslik alus, millele ettevõtted enim tuginesid, on andmesubjekti osalusel sõlmitud lepingu täitmine või vajadus võtta enne lepingu sõlmimist meetmeid (IKÜM artikli 6 lõike 1 punkt b). Seda õiguslikku alust kasutati ka isikuandmete töötlemiseks, mis ei ole lepingu täitmiseks vajalik. Mõne töötlemise puhul oleks õige õiguslik alus õigustatud huvi (IKÜM artikli 6 lõike 1 punkt f). Õigusliku aluse ebaõige kindlaksmääramise tõttu ei ole mõned ettevõtted teinud õigustatud huvide tasakaalustamise testi, mida nõutakse isikuandmete kaitse üldmääruse (IKÜM) artikli 6 lõike 1 punktis f.

2. Andmemaht.

Kuigi taotletud isikuandmete ulatus on klienditi erinev, on ettevõtetele klientidele teenuse osutamiseks vajaliku teabe üldine hulk sarnane. Mõned ettevõtted ei küsi kliendilt eraldi mingit konkreetset teavet, nõudes seega kohustuslikult täidetud teabena väiksemat andmehulka, näiteks ei taotle nad sotsiaalkindlustusnumbrit ega sünniaega. Nimetatud teave saadakse siiski kaudselt, näiteks paludes saata juhiloa foto, mis sisaldab eespool nimetatud andmeid.

Mõnel juhul erineb isikult taotletavate isikuandmete hulk, kui ta soovib teenust saada ja peab taotluse esitama, ettevõtte veebisaitide privaatsuseeskirjades määratletud teenuse saamiseks vajalike andmete hulgast.

3. Läbipaistvus.

Mitmes ettevõttes tuvastati läbipaistvuse põhimõtte mittejärgimine, mis seisnes andmesubjektidele sisulise teabe andmata jätmises. Tuvastati, et:

- ✓ ettevõtte privaatsuspoliitika ja teenusetingimused ei sisalda kogu teavet isikuandmete töötlemise kohta, mis on sätestatud isikuandmete kaitse üldmääruse III peatükis;
- ✓ ettevõtte privaatsuspoliitikas ega teenusetingimustes ei ole täpsustatud, millal kontrollitakse/võidakse kontrollida kliendi juhtimisõigust tõendavaid dokumente, et kontrollida kliendi juhiloa kehtivust;
- ✓ uurimise käigus leiti, et ettevõtted eristavad töötlemisdokumentides kahtlasi kliente, kuid teavet klientide kahtlaseks liigitamise kohta ei ole esitatud ei privaatsuspoliitikas ega Enterprise'i teenusetingimustes. Teatavates olukordades oli järelevalveasutusele esitatud teave puudulik ega vastanud Enterprise'i privaatsuspoliitikas ja teenusetingimustes avaldatud teabele.

4. Säilitamisperioodid.

Kuigi enamikul juhtudel ei leitud selles aspektis vastuolusid isikuandmete töötlemisel, olid ettevõtete märgitud säilitamisperioodid mõnel juhul kindlasti liiga ebamäärased (näiteks säilitatakse andmeid nii kaua, kui see on kohaldatava õiguse kohaselt vajalik või lubatud, või privaatsusavalduse eesmärkide saavutamiseks). Seetõttu ei ole vastuste ja avalikult kättesaadava teabe põhjal selge, kui kaua ja mis põhjustel teatavat liiki andmeid säilitatakse. Mõnes ettevõttes leiti ebakõlasid tehnilistes nõuetes, mis on teataval määral seotud säilitamisperioodiga. Nimelt ei kustutatud klientide isikuandmeid teatavatel kindlaksmääratud tingimustel. Kuigi mittevastavus on kõrvaldatud, ei tekiks selliseid olukordi, kui Enterprise oleks võtnud kõik vajalikud tehnilised meetmed, et tagada andmetöötluse vastavus õigeaegselt, sealhulgas töötlemistoimingute perioodiline läbivaatamine.

5. Biomeetrilised andmed

Ettevõtete vastuseid arvesse võttes võib järeldada, et enamikul juhtudel toimub klientide tuvastamine ja isikuandmete edasine töötlemine biomeetrilisi andmeid kasutamata.

Mõnel juhul töödeldakse kliendi näokujutise andmeid (muude andmete hulgas) isikusamasuse kinnitamiseks siiski andmesubjekti nõusolekul (IKÜM artikli 9 lõike 2 punkt a). Isikuandmete kaitse üldmääruse (IKÜM) artikli 7 nõuete täitmiseks ja selle tagamiseks, et nõusolek antakse vabatahtlikult ja andmesubjektil on nõusoleku andmisel valikuvõimalused, lisavad ettevõtted privaatsuspoliitikasse teabe võimaluse kohta biomeetrilisi andmeid mitte kasutada, st kliendid saavad ettevõttega ühendust võtta, kes saab pakkuda biomeetriliste andmete alternatiivi. Ent ei Enterprise'i kasutustingimused ega privaatsuspoliitika ei paku klientidele samaväärset, vabalt valitud alternatiivi, mis võimaldab biomeetrilisi andmeid mitte kasutada.

VI. SOOVITUSED

1. Sobiva õigusliku aluse kindlaksmääramine.

Isikuandmete kaitse üldmääruse (IKÜM) artikli 6 lõike 1 punkti b tuleb tõlgendada kitsalt ja kitsamalt. Seda ei kohaldata juhtudel, kui töötlemine ei ole vajalik lepingu täitmiseks, kuid ettevõte määrab selle ühepoolselt ettevõtte huvide täitmiseks. Lisaks ei tähenda asjaolu, et osa andmetöötlusest on lepinguga hõlmatud, seda, et selline töötlemine on lepingu täitmiseks vajalik. Näiteks ei ole artikli 6 lõike 1 punkt b sobiv õiguslik alus kliendiprofiili koostamiseks või kommertsteadaannete saatmiseks. Isegi kui sellised töötlemistoimingud on lepingu trahvitrükis eraldi välja toodud, ei tähenda see, et andmetöötlus on lepingu täitmiseks vajalik.

Teisest küljest tuleks juhul, kui töötlemist ei peeta lepingu täitmiseks vajalikuks ja teenust saab osutada ilma konkreetset töötlemist teostamata, määrata kindlaks muu õiguslik alus. Ettevõtjad võivad pärast iga töötlemise laadi hindamist kasutada muud isikuandmete kaitse üldmääruses (IKÜM) ette nähtud õiguslikku alust, näiteks õigustatud huvi (artikli 6 lõike 1 punkt f) või nõusolekut (artikli 6 lõike 1 punkt a), kui asjakohased tingimused on täidetud.

Isikuandmete kaitse üldmääruse (IKÜM) artikli 6 lõike 1 punkt f (isikuandmete töötlemine on vajalik vastutava töötleja või kolmanda isiku õigustatud huvides, välja arvatud juhul, kui andmesubjekti huvid või põhiõigused ja -vabadused, mis nõuavad isikuandmete kaitset, on sellistest huvidest olulisemad, eelkõige juhul, kui andmesubjekt on laps) hõlmab olukordi, kus töötlemine on kaudselt seotud sellise lepingu täitmisega, mille osaline andmesubjekt on.

Sõidukite rentimise kontekstis võib selleks olla sõiduki asukoha (GPS) töötlemine, andmed sõidukipargi jälgimiseks ja varguste vältimiseks. GPSi kasutamine sõltub aga erinevast õiguslikust alusest, sõltuvalt andmetöötluse eesmärgist. Näiteks võiks kohaldada isikuandmete kaitse üldmääruse (IKÜM) artikli 6 lõike 1 punkti b, et teha kindlaks kliendi isik, kes on rikkunud liikluseeskirju ja sellest

tulenevalt lepingut. Isikuandmete kaitse üldmääruse (IKÜM) artikli 6 lõike 1 punktis c viidatakse ka ettevõtte kohustusele esitada haldusrikkumise korral isikuandmeid. GPS-i kasutamine kliendi seadmes kuulub artikli 6 lõike 1 punkti a alla, kui andmetöötluse eesmärk on tagada kliendile täpsed vahemaad tema asukohast sõidukini.

Kui kliendi biomeetrilisi andmeid töödeldakse nõusoleku alusel, tuleb arvesse võtta kehtiva nõusoleku elemente.[1] Andmesubjekti „nõusolek" – vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus, millega andmesubjekt kas avalduse vormis või selge nõusolekut väljendava tegevusega nõustub tema kohta käivate isikuandmete töötlemisega (IKÜM artikli 4 punkt 11). Muu hulgas tuleb märkida, et element „tasuta" tähendab andmesubjektide jaoks tegelikku valikuvõimalust ja kontrolli. Üldreeglina on isikuandmete kaitse üldmääruses (IKÜM) sätestatud, et kui andmesubjektil ei ole tegelikku valikut, ta tunneb, et on sunnitud andma oma nõusoleku, või kui ta peab taluma negatiivseid tagajärgi, kui ta nõusolekut ei anna, siis nõusolek ei kehti.[2] Tuleks märkida, et nõusoleku vabatahtlikkuse tagamiseks peaks vastutav töötleja pakkuma alternatiivset, mitte liiga koormavat isikusamasuse kontrollimise meetodit.

Alljärgnevas tabelis on esitatud kokkuvõte kõige sagedamini leitud isikuandmetest ning isikuandmete töötlemise eesmärkidest ja nende võimalikest õiguslikest alustest. Pange tähele, et iga olukorda tuleb hinnata eraldi ja kõige sobivam õiguslik alus võib erinevates olukordades erineda.

[1] Vt Euroopa Andmekaitsenõukogu suunised 05/2020 määruse (EL) 2016/679 kohase nõusoleku kohta.
[2] Vt Euroopa Andmekaitsenõukogu suunised 05/2020 määruse 2016/679 põhjenduse 13 kohase nõusoleku kohta.

Isikuandmed	**Õiguslik alus (isikuandmete kaitse üldmääruse artikkel 6)**
Isikuandmed (ees- ja perekonnanimi, isikukood / isikukood, sünniaeg), näokujutis (biomeetrilised andmed)	Artikli 6 lõike 1 punkt b – isiku tuvastamine lepingu sõlmimise eesmärgil Artikli 9 lõike 2 punkt a – näotuvastusvahendi kasutamine
Asukohaandmed (GPS-andmed)	Artikli 6 lõike 1 punkt f Parkla jälgimine, varguse ärahoidmine Artikli 6 lõike 1 punkt b Teha kindlaks liikluseeskirjade rikkumise toime pannud ja sellest tulenevalt lepingut rikkunud kliendi isik Artikli 6 lõike 1 punkt c Isikuandmete esitamise kohustus haldusrikkumise korral Artikli 6 lõike 1 punkt a Pakkuda kliendile täpseid vahemaid tema asukohast sõidukiteni
Elukoha postiaadress (linn, tänav, maja nr, korter nr.)	Artikli 6 lõike 1 punkt b Ametlike teadete saatmiseks
Kontaktandmed (telefoninumber, e-posti aadress)	Artikli 6 lõike 1 punkt b Teabevahetuseks, mis on seotud lepingu täitmisega (nt uutest olemasolevatest sõidukitest teavitamine, muudatused maksepoliitikas jne) Artikli 6 lõike 1 punkt f Suhtluseks, et vähendada kiiruseületamisest tingitud liiklusõnnetuste arvu (automaatkõned klientidele, kes ületavad kiirusepiirangut) Artikli 6 lõike 1 punkt a Äriliste teadaannete saatmine
Juhiloa andmed (foto, juhiloa number, aegumiskuupäev, praegused juhiloakategooriad)	Artikli 6 lõike 1 punkt b Kontrollida isiku juhtimisõigust ja kehtivaid juhtimisõiguse kategooriaid
Teave saadud haldusrikkumiste kohta	Artikli 6 lõike 1 punktid b, c ja f Huvide kaitseks ja lepingutingimuste haldamiseks
Teave sõlmitud lepingu kohta (tähtajaline leping, valitud teenus, tingimused)	Artikli 6 lõike 1 punkt b

	teenust osutavate lepinguliste suhete kontrollimiseks ja haldamiseks ning pärast teenuse osutamise lõppu seoses olukordadega, mis võivad tekkida pärast teenuse osutamise perioodi lõppu
Teave liiklusõnnetuste kohta	Artikli 6 lõike 1 punkt f Huvide kaitseks, õnnetuste hindamiseks, teenuse kvaliteedi parandamiseks, kindlustushüvitise taotlemiseks
Arveldus-/makseandmed Kaardiomaniku ees- ja perekonnanimi, kaardi number, aegumiskuupäev ja CVC number	Artikli 6 lõike 1 punkt b Osutatud teenuse eest tasu saamiseks Artikli 6 lõike 1 punkt c Maksevoo tagamiseks

2. Andmete maht

Andmete minimeerimine peaks toimuma isikuandmete töötlemise varases etapis, kogumata andmeid, millest võib loobuda. Kindlaksmääratud eesmärki on vaja rakendada minimaalse andmehulgaga, mis on vajalik selle saavutamiseks. See tähendab, et ei tohi koguda rohkem andmeid, kui on vajalik teenuse osutamiseks.

Sobiva andmehulga kindlaksmääramisel tuleks arvesse võtta järgmisi punkte:

- ✓ töödeldavad isikuandmed peavad olema piisavad ega tohi olla ülemäärased, võttes arvesse nende töötlemise eesmärke;
- ✓ teatavad andmesisestusväljad tuleks välja töötada nii, et need ei jätaks üleliigset ruumi ebavajalike andmete sisestamiseks;
- ✓ ebavajalikud isikuandmed tuleb kustutada pärast määratud aja möödumist;
- ✓ perioodiliselt tuleb kontrollida töödeldavate isikuandmete hulka ja nende vajalikkust.

3. Läbipaistvus

Võttes arvesse isikuandmete kaitse üldmääruses (IKÜM) sätestatud läbipaistvuse põhimõtet, peab vastutav töötleja tagama isikuandmete töötlemise, mis võimaldab andmesubjektil mõista, milliseid andmeid, millisel eesmärgil ja millisel õiguslikul alusel töödeldakse.

Andmesubjektidel peab olema juurdepääs kogu teabele nende isikuandmete kogumise, kasutamise, vaatamise või muul viisil töötlemise kohta ning selle kohta, millises ulatuses isikuandmeid töödeldakse või hakatakse töötlema. Läbipaistvuse põhimõte põhineb nõudel, et kogu teave ja kogu teabevahetus, mis on seotud nimetatud isikuandmete töötlemisega, on kergesti kättesaadav ja arusaadav ning et tuleb kasutada selget ja lihtsat keelt. Nimetatud põhimõtet kohaldatakse eelkõige

andmesubjektide teavitamise suhtes vastutava töötleja identiteedist ja töötlemise eesmärkidest, samuti lisateabe suhtes, et tagada asjaomaste füüsiliste isikute jaoks õiglane ja läbipaistev töötlemine ning nende õigus saada kinnitus ja teade selle kohta, milliseid nende isikuandmeid töödeldakse. Üksikisikuid tuleks teavitada isikuandmete töötlemisega seotud ohtudest, eeskirjadest, kaitsemeetmetest ja õigustest ning sellest, kuidas kasutada sellise töötlemisega seotud õigusi.

Läbipaistvuse põhimõtte rakendamiseks kooskõlas isikuandmete kaitse üldmääruse (IKÜM) nõuetega peab vastutav töötleja tegema järgmist:

- ✓ teave isikuandmete töötlemise kohta peab olema kasutajale kergesti kättesaadav ja kergesti arusaadav selges ja lihtsas keeles. Teave peab olema kättesaadav selle riigi keeles, kus vastutav töötleja tegutseb. Kui neid on mitu, siis kõigis riigikeeltes. Kui haldur tegutseb mitmes riigis, peab teave olema kättesaadav iga riigi riigikeeles;
- ✓ privaatsuspoliitikas nimetatud teave peab vastama vastutava töötleja poolt isikuandmete koguse, eesmärkide ja õiguslike aluste osas praktikas teostatavale töötlemisele. Privaatsuspoliitikas täpsustatud teave peab kajastama vastutava töötleja praktilist käitumist ja andmetega tehtud toiminguid. Kui töötlemistoimingud muutuvad, tuleb privaatsuspoliitikat vastavalt muuta;
- ✓ privaatsuspoliitikas tuleks sellist teavet täpsustada, mis võimaldaks andmesubjektil täielikult mõista, kes on vastutav töötleja, milliseid andmeid töödeldakse, millised on töötlemise eesmärgid ja õiguslik alus, kuidas andmesubjekt saab oma õigusi kasutada. Põhiteave peaks olema järgmine:
    - ettevõtte nimi ja kontaktandmed;
    - andmekaitsespetsialisti kontaktandmed (märkida tuleb e-posti aadress, kus vastutava töötlejaga saab ühendust võtta andmekaitset puudutavate küsimuste või andmesubjekti andmetega tutvumise taotluse korral);
    - töötlemise eesmärk;
    - töödeldavate andmete liigid;
    - töötlemise õiguslik alus (üks isikuandmete kaitse üldmääruse artikli 6 lõikes 1 sätestatud õiguslikest alustest);
    - andmete kogumise allikas;
    - andmesaajad või nende kategooriad;
    - andmete säilitamise aeg/nõuded;
    - kas andmed saadetakse kolmandatele riikidele või rahvusvahelistele organisatsioonidele;
    - juhised isikuandmete kustutamiseks.

- ✓ Privaatsuspoliitikas sisalduvat teavet tuleb regulaarselt ajakohastada, see peab vastama ettevõttes toimuvale isikuandmete töötlemisele;
- ✓ privaatsuspoliitika tuleks avaldada veebisaidil või rakenduses kergesti ligipääsetavas kohas.

4. Andmete säilitamise aeg

Iga isikuandmete töötlemise periood peaks olema selge, õiguspärane ja kindlaks määratud juba isikuandmete kogumise ajal. Vaja oleks hinnata andmete säilitamise kestust, tagades, et isikuandmete säilitamise aeg on rangelt piiratud miinimumiga. Isikuandmed peaksid sisaldama ainult seda, mis on vajalik selle eesmärgi täitmiseks, milleks neid töödeldakse. Andmetöötluse ebakõlade õigeaegseks tuvastamiseks peaksid ettevõtted korrapäraselt läbi vaatama oma sisemiste andmetöötluspõhimõtete asjakohasuse töötlemistoimingute suhtes. See on eriti oluline juhul, kui on toimunud töötlemistoimingud või on alanud töötlemine uuel eesmärgil. Sama kehtib ka tehniliste meetmete kohta, st nende asjakohasus tuleks korrapäraselt läbi vaadata, võttes arvesse olemasoleva tehnoloogia praegust arengut.

Samuti ei ole vähem oluline töötajate iga-aastane koolitus isikuandmete töötlemise valdkonnas. Kvalifitseeritud ja asjatundlik töötaja suudab õigeaegselt tuvastada andmetöötluse ebakõlad ja need kõrvaldada. Lisaks aitab töötajate regulaarne koolitamine töötajatel järgida oma töös isikuandmete töötlemise põhimõtteid, mis võimaldab ettevõtjatel pikas perspektiivis vältida rahalist ja/või mainekahju.

Säilitamise põhimõtte rakendamiseks kooskõlas isikuandmete kaitse üldmääruse (IKÜM) nõuetega peab vastutav töötleja tegema järgmisi toiminguid:

- ✓ isikuandmeid ei tohiks säilitada kauem, kui on vaja selle eesmärgi täitmiseks, milleks neid töödeldakse;
- ✓ tuleb kehtestada asjakohased mehhanismid (eeskirjad, menetlused) isikuandmete automaatseks kustutamiseks;
- ✓ kui see ei ole võimalik ja andmed kustutatakse käsitsi, tuleks korrapäraselt kontrollida andmete kustutamise tähtaegadest kinnipidamist;
- ✓ isikuandmete säilitamise tingimuste/vajaduse perioodiline läbivaatamine (maksimaalne ajavahemik);
- ✓ töötajatele tuleb pakkuda iga-aastast koolitust isikuandmete töötlemise valdkonnas;
- ✓ turvaseaded ja juurdepääsuõigused tuleb korrapäraselt läbi vaadata;

- ✓ tuleb kehtestada selged ja arusaadavad säilitamisperioodid. Kui säilitamistähtaeg on määratletud õigustloovas aktis, tuleb privaatsuspoliitikas osutada konkreetsele tähtajale.

5. Biomeetrilised andmed

Kliendi erikategooria andmete (näokujutise andmete) kasutamisel peab vastutav töötleja tuginema mitte ainult ühele isikuandmete kaitse üldmääruse artiklis 6 sätestatud õiguslikule alusele, vaid ka ühele isikuandmete kaitse üldmääruse artiklis 9 sätestatud erandile erikategooria andmete töötlemise keelust.

Biomeetriliste andmete (näokujutise andmete) kasutamine ettevõtete poolt on õiguslikult võimalik ainult asjakohase selgesõnalise nõusoleku korral. Sõnaselge nõusolek on üks eranditest andmete eriliikide töötlemise keelust. Selleks et andmesubjekti antud nõusolek oleks kehtiv, peab see siiski vastama isikuandmete kaitse üldmääruse artikli 7 sätetele. See tähendab, et nõusolek peab olema:

- ✓ vabalt antud
- ✓ konkreetsel eesmärgil
- ✓ tahtlik ja teadlik
- ✓ andmesubjekti ühemõtteline tahteavaldus, millega andmesubjekt annab selge nõusolekut väljendava tegevuse vormis nõusoleku oma isikuandmete töötlemiseks.

Andmesubjektidel peaks olema tegelik valik ja kontroll oma andmete üle. Juhul kui andmesubjektil ei ole tegelikku valikuvõimalust, kui ta leiab, et nõusolekut sunnitakse või et selle andmata jätmine toob kaasa negatiivsed tagajärjed, ei ole nõusolek kehtiv. Kui nõusolek on lisatud tingimuste mittekaubeldava osana, ei ole see vabatahtlik.

Seetõttu peab ettevõtetel olema võimalik tagada, et nõusolek antakse vabatahtlikult ja on olemas reaalne alternatiiv, mida saab kasutada juhtudel, kui andmesubjekt ei soovi nõusolekut anda või on selle tagasi võtnud. Biomeetriliste andmete alternatiivse kasutamise näitena kaaluvad institutsioonid dokumentide vahetut kontrollimist või videokõnede kontrollimist.

Ametiasutused ei välista muid alternatiive, kuid rõhutavad, et sellistel juhtudel on oluline tagada, et see ei tekitaks ülemäära suurt haldus- või muud koormust, mõjutades seega andmesubjekti nõusolekut andma.