

RREGULLORE
PËR PËRPUNIMIN, MBROJTJEN, RUAJTJEN DHE SIGURINË E TË DHËNAVE
PERSONALE

Kontrolluesi: Shoqëria "AEDistribution" shpk
Data e hyrjes në fuqi: 10.02.2025
Versioni: 1.0
Përgjegjës për zbatimin: Punonjësit dhe personi i ngarkuar për mbrojtjen e të dhënave (DPO)

1. QËLLIMI I RREGULLORES

Qëllimi i kësaj rregulloreje është të përcaktojë rregullat, masat dhe procedurat për përpunimin, ruajtjen, sigurinë dhe mbrojtjen e të dhënave personale dhe sensitive që përpunohen nga shoqëria "AEDistribution" shpk, në përputhje me legjislacionin në fuqi për mbrojtjen e të dhënave personale.

2. FUSHA E ZBATIMIT

Kjo rregullore zbatohet për:

- Punonjësit e shoqërisë në të gjitha nivelet
- Klientët
- Bashkëpunëtorë dhe konsulentë të jashtëm
- Personelin e kontraktuar dhe çdo palë e tretë që ka akses në të dhënat
- Studentët në praktikë
- Audituesit dhe inspektuesit e jashtëm

2. BAZAT LIGJORE

- Ligji nr. 124/2024 "Për mbrojtjen e të dhënave personale"
- Udhëzimi nr. 2/2025 për të dhënat personale shëndetësore
- Udhëzimi nr. 47/2018 për SMSI (Sistemin e Menaxhimit të Sigurisë së Informacionit)
- Udhëzimi nr. 19/2012 për marrëdhënien kontrollues-përpunues
- Udhëzimi nr. 42/2012 "përpunimin e të dhënave personale të kandidatëve për punë"
- Vendimi nr. 6 i Komisionerit për sigurimin e të dhënave
- Ligji nr. 87/2019 "Për faturën dhe sisteminin e monitorimit të qarkullimit"

4. KATEGORITË E TË DHËNAVE QË PËRPUNOHEN

4.1 Të dhëna identifikuese

- Emër, mbiemër, datëlindje,
- Numri i dokumentit të identitetit/ID
- Adresa e banimit dhe e punës
- Numri i telefonit dhe email-i

4.2 Të dhëna të punësimit

- CV dhe dokumentacioni i kualifikimeve
- Kontrata dhe shtojca
- Vlerësime të performancës
- Leje mjekësore dhe pushime
- Të dhëna për pagat dhe sigurimet

4.3 Të dhëna CCTV

- Video- të ambienteve të brendshme

- Video- të hyrjeve dhe daljeve
- Pamje të zonave private

4.4 Të dhëna teknike

- Adresë IP dhe log-e të sistemit
- Përdorim i softuerit të shoqërisë
- Akses në databaza dhe sisteme elektronike
- Komunikime elektronike

5. PARIMET E PËRPUNIMIT

5.1 Ligjshmëria dhe Transparenca

Përpunimi bëhet vetëm me bazë ligjore të qartë dhe subjektet informohen në mënyrë transparente.

5.2 Qëllim i përpunimit

Të dhënat përdoren vetëm për qëllimet e deklaruar dhe të ligjshme.

5.3 Minimizim i të dhënave

Përpunohen vetëm të dhënat që janë të nevojshme dhe relevante.

5.4 Saktësia e të dhënave që përpunohen

Të dhënat mbahen të sakta dhe përditësohen rregullisht.

5.5 Koha e ruajtjes së të dhënave

Të dhënat ruhen vetëm për kohën e nevojshme që lidhet me qëllimin e përpunimit, sipas afateve të përcaktuara.

5.6 Siguria dhe konfidencialitet

Zbatohen masa të përshtatshme teknike dhe organizative sipas akteve të miratuara.

5.7 Llogaridhënie dhe dokumentim

Mbahen regjistrime të detajuara për çdo veprimtari përpunimi sipas regjistrimit të disponuar nga DPO.

6. TË DREJTAT E SUBJEKTEVE TË TË DHËNAVE

6.1 E drejta për informim

Çdo subjekt (Klient/ punonjës /vizitor) ka të drejtë të:

- Njihet me të dhënat e kontrolluesit
- Mësojë qëllimet e përpunimit
- Informohet për kategorinë e të dhënave
- Mësojë afatin e ruajtjes
- Me të drejtat e tij

6.2 E drejta e aksesit

- Konfirmim nëse të dhënat përpunohen
- Kopje të të dhënave personale
- Informacione për burimin e të dhënave
- Qëllimet e përpunimit
- Kategoritë e marrësve
- Marrje e të dhënave në format elektronik

- Transferim tek kontrollues tjetër
- Transmitem i drejtpërdrejtë kur është e mundur

6.3 E drejta për korrigjimin e të dhënave

- Korrigjim i të dhënave të pasakta
- Plotësim i të dhënave të munguara
- Përditësim i informacioneve të vjetruara

6.4 E drejta për fshirjen e të dhënave

- Fshirje kur nuk janë më të nevojshme
- Tërheqje e pëlqimit
- Përpunim i paligjshëm
- Kundërshtim me ligjshëm

6.5 E drejta për kufizimin e përpunimit

- Kufizim i përpunimit gjatë verifikimit
- Kufizim deri në zgjidhjen e ankesave
- Ruajtje vetëm për qëllime specifike

6.6 E drejta për kundërshtimin e përpunimit

- Kundërshtim për qëllime të ligjshme
- Kundërshtim për marketing direkt
- Kundërshtim për profilezim

7. MASAT PËR SIGURINË E TË DHËNAVE

7.1 Masa teknike

7.1.1 Kontrolli i aksesit

- Sisteme identifikimi me përdorues dhe fjalëkalime
- Autentifikim me dy faktorë për sisteme që përpunojnë të dhënat e klientëve kur bëhet “on-line”
- Kartela aksesi për zona të kufizuara
- Rregjistër aksesi
- Urdhëra nga eprori

7.1.2 Mbrojtja e të dhënave

- Enkriptim i të dhënave në ruajtje dhe transmetim
- Kopje rezervë të bazës së të dhënave
- Sisteme për vazhdimësi
- Testim periodik i rikuperimit

7.1.3 Siguria e rrjetit

- Firewall të përditësuar dhe të konfiguruar
- Antiviruse dhe anti-malware
- Monitorim i trafikut të rrjetit
- Segmentim i rrjetit për të dhënat sensitive

7.1.4 Pajisje mobile

- Politika për përdorimin e pajisjeve personale
- Enkriptim i pajisjeve mobile

- Mundësi për fshirje të largët
- Regjistrimi i pajisjeve të autorizuara

7.2 Masa organizative

7.2.1 Menaxhimi i aksesit

- Autorizime me role për personelin
- Rishikim periodik i të drejtave të aksesit
- Procedura për dhënien dhe heqjen e aksesit
- Regjistrim i të gjitha veprimtarive

7.2.2 Politika dhe procedurat

- Politika për përdorimin e sistemeve informatike
- Procedura për raportimin e incidenteve pranë insitucionit përktës
- Udhëzime për trajtimin e të dhënave sensitive
- Procedura për auditimin e brendshëm

7.2.3 Monitorimi dhe mbikqyrja

- Monitorim i hyrjeve në ambientet me të dhëna sensitive
- Regjistrim i aksesit në sisteme
- Raportim i veprimtarive të dyshimta
- Inspektime/audite të rregullta

7.2.4 Trajnimi dhe ndërgjegjësimi

- Trajnime vjetore për të gjithë personelin
- Sesione të specializuara për role specifike
- Testimi i njohurive për sigurinë
- Materialet e trajnimit të përditësuara

8. DEPARTAMENTI I ARKIVËS

8.1 Organizimi i arkivës

8.1.1 Struktura fizike

- Ambiente të sigurta me kontrollin e aksesit
- Sisteme të kontrollit të temperaturës dhe lagështisë
- Mbrojtje nga zjarri dhe uji
- Rafta të organizuara me sistem kodifikimi

8.1.2 Kategorizimi i dokumentave

- Dokumenta aktive (akses i rregullt)
- Dokumenta gjysëmaktive (akses i kufizuar)
- Dokumenta historike/statistika (ruajtje afatgjate)
- Dokumenta për asgjësim

8.2 Procedurat e arkivimit

8.2.1 Pranim i dokumentave

- Verifikimi i plotësisë së dokumentacionit
- Regjistrimi në sistemin e arkivës

- Etiketimi me kode identifikimi
- Vendosja në pozicionin e caktuar

8.2.2 Ruajtja dhe organizimi

- Mbajtja e regjistrave të detajuara
- Indeksimi për kërkim të shpejtë
- Kontrollle periodike të gjendjes
- Mbrojtja nga dëmtimi fizik

8.2.3 Dhënia e dokumentave

- Kërkesë zyrtare për akses
- Verifikimi i autorizimit
- Regjistrimi i dhënies
- Ndjekja e kthimit

8.3 Digitalizimi i arkivës

8.3.1 Procesi i digitalizimit

- Skaninimi me cilësi
- Indeksimi elektronik
- Kontrolli i cilësisë
- Backup-i i të dhënave

8.3.2 Mbrojtja e arkivës digjitale

- Enkriptimi i dosjeve
- Akses me autorizim
- Kopje rezervë të të dhënave
- Auditimi i aksesit

9. BURIMET NJERËZORE

9.1 Politikat e pranimi

9.1.1 Rekrutimi dhe seleksioni

- Verifikimi i dokumentacionit
- Kontrolli i referencave
- Marrëveshje konfidencialiteti

9.1.2 Orientimi i punonjësve të rinj

- Trajnim fillestar për mbrojtjen e të dhënave
- Nënshkrimi i politikave të sigurisë
- Dhënia e aksesit të nevojshëm
- Monitorimi i periudhës së proves

9.2 Menaxhimi i dosjes së punonjësit

9.2.1 Informacioni i ruajtur

- Të dhëna personale bazë
- Dokumentacioni i kualifikimeve
- Kontrata dhe shtojca
- Vlerësime të performancës
- Regjistrime të trajnimeve

9.2.2 Akses në dosjë

- Vetëm personeli i autorizuar
- Punonjësi vetë (me kërkesë)
- Audituesit e brendshëm
- Autoritetet kompetente

9.3 Trajnimi dhe zhvillimi

9.3.1 Programi i trajnimit

- Trajnim fillestar për të gjithë punonjësit
- Trajnim i specializuar për role specifike
- Përditësime të rregullta
- Testimi i njohurive

9.3.2 Dokumentimi i trajnimit

- Regjistri i pjesëmarrjes
- Vlerësimi i performancës
- Certifikimi i kompetencave
- Plani i trajnimit individual

10. REGJISTRIMI I KLIENTËVE

10.1 Procesi i regjistrimit

10.1.1 Mbledhja e të dhënave

- Verifikimi i identitetit
- Plotësimi i formularëve
- Kontrolli i dokumentacionit
- Dhënia e numrit të klientit

10.1.2 Krijimi i kartelës

- Hapja e kartelës elektronike
- Regjistrimi i të dhënave bazë
- Lidhja me sistemin e faturimit
- Aktivizimi i aksesit

10.2 Menaxhimi i kartelës së Klientit

10.2.1 Përmbajtja e kartelës

- Të dhënat e klientit
- Historia klientit
- Shërbime dhe trajtime
- Informacione për statusin aktual

10.2.2 Përditësimi i kartelës

- Përditësimi i informacioneve kontakti
- Regjistrimi i ndryshimeve

10.3 Akses në kartelë

10.3.1 Personeli i autorizuar

- Personeli administrativ (i kufizuar)
 - Specialistë konsultues
- 

10.3.2 Kontrolli i aksesit

- Autentifikim me identifikim
- Regjistrimi i çdo aksesit
- Kufizimi bazuar në rolin
- Monitorimi i veprimtarive

11. DEPARTAMENTI I TEKNOLOGJISË

11.1 Infrastruktura teknike

11.1.1 Sisteme dhe server

- Servera të sigurt me enkriptim
- Sisteme rezervë (backup)
- Monitorimi i disponueshmërisë
- Përditësime të rregullta

11.1.2 Rrjeti dhe komunikimi

- Rrjet i sigurt i brendshëm
- Lidhje të enkriptuara
- Firewall të konfiguruar
- Monitorimi i trafikut

11.2 Siguria e informacionit

11.2.1 Politikat e sigurisë

- Politika për fjalëkalimet
- Procedura për backup
- Menaxhimi i incidenteve
- Kontrolli i aksesit

11.2.2 Monitorimi dhe auditimi

- Log-et e sistemit
- Monitorimi i sigurisë
- Testimi i vulnerabiliteteve
- Raportimi i incidenteve

11.3 Menaxhimi i të dhënave

11.3.1 Ruajtja e të dhënave

- Databaza të sigurta
- Kopje rezervë automatike
- Arkivimi afatgjatë
- Fshirja e sigurt

11.3.2 Integrimi i sistemeve

- Ndërlidhja e sistemeve
- Standardizimi i të dhënave
- Sinkronizimi i informacionit
- Kontrolli i cilësisë

12. RREGULLAT PËR TË DHËNAT PERSONALE



12.1 Ruajtja fizike

- Kartelat fizike ruhen në dollapë të mbyllura me çelës
- Akses i kufizuar në zyra
- Sisteme alarmi për ambientet e ndjeshme
- Kontrolli i hyrjeve dhe daljeve

12.2 Ruajtja elektronike

- Kartelat elektronike mbrohen përmes fjalëkalimeve
- Enkriptimi i të dhënave në databazë
- Auditimi i aksesit dhe veprimtarive
- Kopje rezervë të kriptuara

12.3 Aksesit dhe përdorimi

- Akses të kufizuar vetëm për personelin e autorizuar
- Përpunim vetëm për qëllime të shërbimit të ofruar
- Ndalim i aksesit për kuriozitet personal
- Raportimi i çdo aksesit të paautorizuar

12.4 Transmetimi i të dhënave

- Kanale të sigurta për transmetim
- Enkriptimi i komunikimeve
- Konfirmimi i pranimit
- Auditimi i transmetimeve

13. AFATET E RUAJTJES

13.1 Tabela e afateve

Kategoria e të dhënave	Afati i ruajtjes	Baza ligjore
Kartela pacientësh	5 vjet nga dita e fundit e trajtimit	Ligji për Fiskalizimin
Regjistrimet CCTV	Maksimumi 30 ditë	Ligji për mbrojtjen e të dhënave
Dosjat e punonjësve	6 muaj pas largimit	Kodi i Punës
CV të refuzuara	2 muaj	Ligji për mbrojtjen e të dhënave
Të dhëna kontakti		Ligji për mbrojtjen e të dhënave
Fatura dhe të dhëna financiare	5 vjet	Ligji për kontabilitetin
Dokumenta administrativ	3 vjet	Ligji për arkivat
Regjistrat e trajnimeve	5 vjet	Ligji për arsimin

13.2 Procedura e asgjësimit

13.2.1 Asgjësimi elektronik

- Fshirja e sigurt e të dhënave
- Mbishkrimi i sektorëve të diskut
- Verifikimi i fshirjes
- Regjistrimi i procesit

13.2.2 Asgjësimi fizik

- Copëtimi i dokumentave
- Djegja e kontrolluara
- Asgjësimi i pajisjeve

13.2.3 Dokumentimi

- Regjistri i asgjësimit
 - Aprovimi i autorizuar
 - Dëshmitë e asgjësimit
 - Auditimi i procesit
-

14. PËRPUNIMI NGA PALË TË TRETA (PËRPUNUESIT)

14.1 Kriteret e selektimit

- Vlerësimi i sigurisë
- Certifikime të sigurisë
- Referenca nga klientë të tjerë
- Kapacitetet teknike

14.2 Kontrata e përpunimit

Për çdo përpunues që përpunon të dhëna në emër të shoqërisë, lidhet kontratë specifike që parashikon:

14.2.1 Detyrimet e përpunuesit

- Përpunim vetëm sipas udhëzimeve
- Zbatimi i masave të sigurisë
- Trajnimi i personelit
- Raportimi i incidenteve

14.2.2 Kufizimet

- Mos-transferim tek palë të treta
- Mos-përdorim për qëllime të tjera
- Akses i kufizuar
- Konfidencialiteti i plotë

14.2.3 Përfundimi i bashkëpunimit

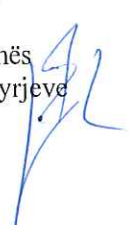
- Kthimi i të dhënave
- Fshirja e kopjeve
- Konfirmimi i asgjësimit
- Auditimi final

14.3 Monitorimi i përpunuesve

- Auditimi i regullt
- Vlerësimi i përputhshmërisë
- Raportimi i performancës
- Masat korrigjuese

15. VIDEO-SURVEJIMI (CCTV)

15.1 Qëllimet e survejimit

- Sigurie e jetës
 - Mbrojtje e pronës
 - Monitorimi i hyrjeve
- 

15.2 Vendosja e kamerave

- Zona publike (korridore)
- Hyrje dhe dalje
- Zona me rrezik të lartë
- Ndalohe në ambiente të postit të punës dhe të kujdesit

15.3 Informimi i subjekteve të të dhënave

- Tabelat informuese sipas modelit të miratuar
- Njoftim për qëllimet e survejimit
- Informacion për kontaktin
- Të drejtat e subjekteve

15.4 Menaxhimi i pamjeve

- Akses vetëm nga persona të autorizuar
- Ruajtja maksimale 30 ditë
- Fshirja automatike
- Regjistrimi i aksesit

15.5 Dhënia e pamjeve

- Kërkesë zyrtare
- Verifikimi i bazës ligjore
- Mbrojtja e privatësisë së palëve të treta
- Dokumentimi i dhënies

16. SHKELJET DHE INCIDENTET

16.1 Kategoritë e incidenteve

- Rrjedhje të dhënash
- Akses i paautorizuar
- Gabim njerëzor
- Sulm kibernetik
- Dëmtim i sistemeve
- Humbje e të dhënave

16.2 Procedura e raportimit bëhet sipas hapave

- Zbulimi i incidentit
- Raportimi i menjëhershëm te DPO
- Vlerësimi i rreziqshmërisë
- Njoftimi i autoriteteve (brenda 72 orëve)
- Njoftimi i subjekteve (kur është e nevojshme sipas ligjit për mbrojtjen e të dhënave personale)

16.3 Menaxhimi i incidenteve bëhet sipas hapave.

- Izolimi i problemit
- Vlerësimi i dëmit
- Masat korrigjuese
- Monitorimi i situatës
- Raportimi final

16.4 Regjistri i incidenteve duhet të përmbajë



- Përshkrimi i incidentit
- Shkaqet e identifikuara
- Masat e marra
- Përfundimet
- Rekomandimet

17. TRAJNIMI I PERSONELIT

17.1 Trajnimi fillestar

- Për çdo punonjës të ri
- Përpara fillimit të punës
- Mbulon të gjitha aspektet

17.2 Trajnimi periodik

- Çdo 12 muaj për të gjithë personelin
- Përditësime për ndryshime ligjore
- Sesione të specializuara
- Trajnim për incident

17.3 Përmbajtja e trajnimit duhet të fokusohet

- Ligji për mbrojtjen e të dhënave
- Politikat e shoqërisë
- Procedurat e sigurisë
- Shembuj praktik
- Detyrimet dhe përgjegjësitë

17.4 Dokumentimi i trajnimit

- Regjistrimi i pjesëmarrjes
- Vlerësimi i performancës
- Certifikimi i kompletimit
- Planifikimi i trajnimit të ardhshëm

17.5 Materialet e trajnimit

- Prezantime interaktive
- Udhëzues praktik
- Studie rasti
- Teste vlerësimi
- Burime referimi

18. AUDITIMI DHE PËRGJEGJËSIA

18.1 Auditimi i brendshëm

- Vlerësimi i përputhshmërisë
- Kontrolli i sistemeve
- Testimi i procedurave
- Identifikimi i mangësive

18.2 Auditimi i jashtëm

- Nga autoritetet kompetente
- Nga auditues të certifikuar
- Nga partnerë kontraktual

18.3 Përgjegjësitë

- | | |
|--------------------------------|----------------------------|
| • Drejtori i Përgjithshëm: | Përgjegjësi e përgjithshme |
| • DPO: | Mbikëqyrja e zbatimit |
| • Menaxherët e departamenteve: | Zbatimi praktik |
| • Punonjësit: | Respektimi i rregullave |

18.4 Masat disiplinore

- Vërejtje me gojë
- Vërejtje me shkrim
- Gjobë deri në 20% të pagës
- Pezullim nga puna
- Largim nga puna

18.5 Rishikimi i rregullores duhet të konsiderohet

- Një herë në 2 vjet
- Pas ndryshimeve ligjore
- Pas incidenteve të rëndësishme
- Bazuar në rekomandimet e auditimit

19. PROCEDURAT E VEÇANTA

19.1 Emergjenca mjekësore

- Akses i shpejtë në të dhëna
- Informim i përfaqësuesit të subjektit të të dhënave
- Koordinim me shërbimet
- Dokumentimi i veprimeve

19.2 Kërkesa ligjore

- Verifikimi i autoritetit
- Kontrolli i dokumentacionit
- Përgjigjia brenda afatit
- Mbikëqyrja e DPO

19.3 Transferimi i të dhënave

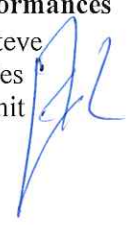
- Pëlqimi i Klientit
- Sisteme të sigurta
- Konfirmimi i pranimit

19.4 Kërkimi shkencor

- Aprovimi i komitetit etik
- Anonimizimi i të dhënave
- Marrëveshje bashkëpunimi
- Publikimi i rezultateve

20. MONITORIMI DHE RAPORTIMI

20.1 Indikatorët e performances

- Numri i incidenteve
 - Koha e përgjigjies
 - Shkalla e trajnimit
- 

20.2 Raportimi i rregullt

- Raport mujor për DPO
- Raport tremujor për drejtorinë
- Raport vjetor për bordin
- Raport për autoritetet

20.3 Përmirësimi i vazhdueshëm

- Analiza e të dhënave
- Identifikimi i problematikave
- Planifikimi i masave
- Implementimi i ndryshimeve

21. DISPOZITA PËRFUNDIMTARE

21.1 Hyrja në fuqi

Kjo rregullore hyn në fuqi menjëherë pas miratimit dhe zëvendëson çdo rregullore të mëparshme.

21.2 Shpërndarja

Rregullorja shpërndahet te të gjithë punonjësit dhe publikohet në faqen e internetit.

21.3 Interpretimi

Çdo mosmarrëveshje në interpretim zgjidhet nga DPO në konsultim me strukturat përkatëse

21.4 Ndryshimet

Ndryshimet bëhen vetëm me aprovin e drejtuesit dhe pas konsultimit me DPO.

Dokument i miratuar nga:

Shoqëria "AEDistribution" shpk
Administratori

Elton Kuka



Personit të Ngarkuar për Mbrojtjen e të dhënave DPO

Ermir Kallaku

Shënim: Ky dokument është i rëndësishëm për të gjithë punonjësit dhe duhet të ruhet në vend të dukshëm. Çdo punonjës duhet të njihet me përmbajtjen dhe të nënshkruajë konfirmimin e leximit dhe kuptimit.

ANEKS NR. 1
PËR ZBATIMIN E RREGULLORES

1. Të dhënat e ruajtura në sistemin e video survejmit (imazhet) përbëjnë të dhëna personale.
2. Përpunimi i këtyre të dhënave nga shoqëria “A.E.Distribution” shpk realizohet vetëm në përmbushje të detyrimit ligjor të parashikuar nga ligji nr. 19/2016 “Për masat shtesë të sigurisë publike”. Të dhënat e regjistruara për këtë qëllim, nuk duhet të përdoren për qëllime të tjera, përveç rasteve që parashikohen me ligj, p.sh. për interesa të rëndësishme publike si lufta kundër krimit.
3. Instalimi dhe përdorimi i sistemeve të videosurvejmit (CCTV), që përpunojnë të dhëna personale, duhet të jenë të vendosura vetëm në ato vende dhe hapsira të cilat mundësojnë realizimin e qëllimit për të cilin janë vendosur, pa cënuar të drejtat themelore të njeriut, si e drejta për jetën private, familjare dhe e drejta për mbrojtjen e të dhënave personale. Për këtë arsye personi i caktuar për mbrojtjen e të dhënave personale pranë shoqërisë duhet të marrë masa që instalimi i sistemit (cctv) të mos çënoj të drejtat e sipërcituara.
4. Është e ndaluar rreptësisht instalimi i një sistemi CCTV, në ambiente që përdoren ekskluzivisht për qëllime private si tualete, dushe, dhoma zhveshje etj.
5. Është e ndaluar rreptësisht shpërndarja e regjistrimeve të ruajtuara në sistemin CCTV që përmbajnë të dhëna personale, me përjashtim të rasteve kur ato kërkohen nga autoritetet e autorizuar dhe në rastet e përcaktuara në ligj.
6. Personi i caktuar për mbrojtjen e të dhënave personale pranë shoqërisë duhet të marrë masa që të dhënat e sistemit CCTV të mos jenë të aksesueshme nga persona të paautorizuar. Për këtë arsye ai duhet të sigurojë që:
 - a) të dhënat duhet të ruhen për një afat sa më të shkurtër të jetë e mundur;
 - b) Vetëm personi i caktuar për mbrojtjen e të dhënave personale pranë shoqërisë, autorizohet të ketë akses në të dhënat e regjistruara.
 - c) çdo akses i marrë prej tij në të dhënat e regjistruara duhet të dokumentohet, për qëllime të një kontrolli të mundshëm të mëvonshëm.
 - ç) Masat e sigurisë duhet të mbrojnë sistemet e regjistrimit dhe pajisjet e transmetimit që ruajnë të dhënat e regjistruara, duke i mbrojtur ato nga aksesit, ndryshimi, shkatërrimi, humbja ose përpunimi i paautorizuar ose aksidental
7. Përpara fillimit të përpunimit të të dhënave personale me anë të sistemit CCTV, duhet të merret dhe të dokumentohet me një akt të brendshëm nga organi vendimmarrës i kontrolluesit, duke përcaktuar pikat e mëposhtme:
 - a) llojin, specifikimet e kamerave dhe vendosjen e tyre në përputhje me qëllimin për të cilin do të përdoren. Pozicioni i kamerave nuk duhet të jetë në një mënyrë, nga e cila përftohen imazhe nga mjedise që nuk përputhen me qëllimin e mbikëqyrjes;
 - b) zonat e sakta që do të jenë nën mbikëqyrje; p.sh. ndalohet monitorimi dhe regjistrimi i imazheve në ambiente private;

- c) ndalohet mbikëqyrja dhe transmetimi në kohë reale i imazheve të regjistruara nga sistemi CCTV, nëpërmjet internetit ose shërbimeve të komunikimit elektronik, ku personat mund të identifikohen lehtë.
8. Afati i ruajtjes së të dhënave të regjistruara, nuk duhet të kalojë periudhën e nevojshme, për përmbushjen e qëllimit, për të cilin janë regjistruar këto të dhëna. Të dhënat mund të mbahen:
- a) për një periudhë prej 72 orësh
 - b) për një periudhë më të gjatë, nëse mjediset e kontrolluara nuk janë nën mbikëqyrje të vazhdueshme, megjithatë, jo më shumë se 30 ditë
 - c) për periudha më të gjata kur parashikohet me akt normativ/rregullator të posaçëm.
9. Pas përfundimit të periudhës së ruajtjes së regjistrimeve, personi i caktuar për mbrojtjen e të dhënave personale pranë shoqërisë realizon fshirjen e këtyre të dhënave.
10. Në rast të një incidenti sigurie, personi i caktuar për mbrojtjen e të dhënave personale pranë shoqërisë, duhet t'i vendosi në dispozicion Autoriteteve Kompetente në kuptim të Ligjit, të dhënat e sistemit CCTV.
11. Personi i caktuar për mbrojtjen e të dhënave personale pranë shoqërisë është i detyruar të vendosë në ambientet e survejuara me kamera, modelin standard të tabelës informuese për mbikëqyrjen me sistemin CCTV, të miratuar nga Komisioneri.
12. Të dhënat personale, të përftuara nga sistemi I videosurvejimit duhet të mbahen në mënyrë të sigurt dhe të mos keqpërdoren apo cenohen nga persona të paautorizuar. Siguria nuk lidhet vetëm me masat e sigurisë fizike, por gjithashtu me organizimin e punës në mënyrë të tillë që të minimizohet rreziku, për shembull, duke siguruar që personeli të ketë akses në të dhënat personale vetëm për aq sa është e nevojshme për të kryer veprimtarinë e tyre të punës. Çdo punonjës duhet të trajnohet rregullisht mbi përdorimin e sigurt të të dhënave personale dhe të kuptojë qartë përgjegjësitë dhe kufizimet që ka, në përputhje me kërkesat e Ligjit.
13. Kontrolluesit, përpunuesit dhe personat e autorizuar, të cilët gjatë ushtrimit të detyrës, vihen në dijeni për përmbajtjen e të dhënave të regjistruara nga sistemi CCTV, janë të detyruar ta ruajnë konfidencialitetin edhe pas përfundimit të punës së tyre, për kontrolluesin ose përpunuesin.
14. Personi i caktuar për mbrojtjen e të dhënave personale duhet të marri masat që të gjitha të drejtat e subjektit të të dhënave, duhet të garantohen, në përputhje me parashikimet e neneve 13 deri në 20 të Ligjit, veçanërisht e drejta për akses, e drejta për të kundërshtuar dhe e drejta për fshirje. Nëse një subjekt i të dhënave kërkon akses në të dhënat e tij të video-survejimit, këto të dhëna nuk mund të fshihen pas marrjes së kësaj kërkesë. Në rast se dhënia e aksesit do të përmbushet duke i treguar subjektit të të dhënave materialin e regjistruar, duhet të merren parasysh interesat e mbrojtjes së të dhënave të palëve të treta, duke bërë të mundur anonimizimin e videos duke errësuar imazhin e tyre.
15. Personi i caktuar për mbrojtjen e të dhënave personale përcakton dhe zbaton masat e duhura teknike dhe organizative për të siguruar një nivel sigurie të përshtatshëm ndaj rrezikut, duke përfshirë, ndër të tjera, kur është e zbatueshme:
- a) pseudonimizimin dhe enkriptimin e të dhënave personale;

- b) aftësinë për të garantuar konfidencialitetin, integritetin, disponueshmërinë dhe qëndrueshmërinë e sistemeve dhe të shërbimeve të përpunimit;
 - c) aftësinë për të rivendosur disponueshmërinë dhe aksesin në të dhënat personale brenda një kohe të arsyeshme në rast incidenti fizik ose teknik;
 - ç) një proces për testimin, shqyrtimin dhe vlerësimin e rregullt të efikasitetit të masave teknike dhe organizative për të garantuar sigurinë e përpunimit.
16. Personi i caktuar për mbrojtjen e të dhënave personale, duhet të kryejë vlerësimin e përshtatshmërisë të nivelit të sigurisë, duke marrë në konsideratë rreziqet që shkaktohen nga përpunimi, specifikisht, nga shkatërrimi aksidental ose i paligjshëm, humbja, ndryshimi, përhapja e paautorizuar ose aksesin në të dhënat personale të transmetuara, të ruajtura ose të përpunuara në çfarëdolloj mënyre.
- 17 Personi i caktuar për mbrojtjen e të dhënave personale, duhet të hartojë dhe zbatojë kodin e sjelljes, me qëllim sigurimin që çdo person që vepron në autoritetin e shoqërisë "AEDistribution shpk dhe që ka akses në të dhënat personale, të mos i përpunojë ato në kundërshtim me udhëzimet e shoqërisë, me përjashtim të rastit kur kërkohet nga legjislacioni në fuqi.

Dokument i miratuar në 06.05.2025 nga:

**Shoqëria "AEDistribution" shpk
Administratori**

Elton Kuka



**Personit të Ngarkuar për Mbrojtjen e të
dhënave DPO**

Ermir Kallaku

Shënim: Ky dokument është i rëndësishëm për të gjithë punonjësit dhe duhet të ruhet në vend të dukshëm. Çdo punonjës duhet të njihet me përmbajtjen dhe të nënshkruajë konfirmimin e leximit dhe kuptimit.