Tel: + 355 4 2 269097
Fax : + 355 4 2 269325
E-Mail: info@dpa.gov.al



**Udhëzues në lidhje me akreditimin sipas skemave ISO/IEC 27017 ( Teknologjia e informacionit – Teknikat e sigurisë — Kod praktike për kontrollet e sigurisë së informacionit bazuar në ISO/IEC 27002 për shërbimet në platforma 'cloud') dhe ISO/IEC 27018 ( Teknologjia e informacionit – Teknikat e sigurisë — Kod praktike për mbrojtjen e informacionit të identifikimit të personave (PII) në platforma publike 'cloud' që veprojnë si përpunues të PII-ve), si shtesa mbi skemën e certifikimit ISO/IEC 27001.**

**Zbatues:** Stafi i DPA-së, të gjitha Organet e Vlerësimit të Konformitetit të akredituara dhe aplikantët

**Përgjegjës për zbatim:** Drejtori i Drejtorisë së Organeve Certifikuese dhe Inspektuese

Kontrolloi: Ardita MELE
Menaxheri i Cilësisë

Miratoi: Pranvera FAGU
Drejtori i Përgjithshëm

## 1. QËLLIMI

Ky dokument përshkruan udhëzime për akreditimin sipas ISO/IEC 27017 dhe ISO/IEC 27018 (të dyja së bashku të konsideruara si një skemë e vetme). Ky dokument është i vlefshëm për DPA dhe vlerësuesit e saj si dhe për organet certifikuese të sistemeve të menaxhimit të sigurisë së informacionit të akreditуar nga DPA, organet certifikuese të sistemeve të menaxhimit të sigurisë së informacionit që kanë aplikuar për akreditim apo që kanë për qëllim të aplikojnë për akreditim.

## 2. FUSHA E ZBATIMIT

Ky udhëzues zbatohet nga vlerësuesit dhe stafi i DPA, nga nënkontraktuesit e saj për vlerësimin e organeve certifikuese që kryejnë certifikim të sistemeve të menaxhimit të sigurisë së informacionit në përputhje me këtë standard.

## 3. PËRGJEGJËSITË

Ky udhëzues është pjesë e sistemit të menaxhimit të DPA dhe si i tillë është nën përgjegjësinë e Drejtorit të Drejtorisë së Zhvillimit rishikimi i vazhdueshëm në varësi të ndryshimeve të duhura dhe përmirësimeve të vazhdueshme në sistemin e menaxhimit të DPA. Është detyrë e Drejtorit të Drejtorisë së organeve certifikuese dhe inspektuese të kontrollojë zbatimin e këtij udhëzimi.

## 4. REFERENCA

ISO/IEC 27017:2015, Teknologjia e informacionit – Teknikat e sigurisë — Kod praktike për kontrollet e sigurisë së informacionit bazuar në ISO/IEC 27002 për shërbimet në platforma 'cloud'.

ISO/IEC 27018:2019, Teknologjia e informacionit – Teknikat e sigurisë — Kod praktike për mbrojtjen e informacionit të identifikimit të personave (PII) në platforma publike 'cloud' që veprojnë si përpunues të PII-ve.

ISO/IEC 27001:2022, Teknologjia e informacionit – Teknikat e sigurisë – Sistemet e menaxhimit të sigurisë së informacionit – Kërkesat.

ISO/IEC 27006:2015, Teknologjia e informacionit – Teknikat e sigurisë – Kërkesa për organe ofruese të vlerësimit dhe certifikimit të sistemeve të menaxhimit të sigurisë së informacionit.

ISO/IEC 27006:2015, Amendim 1:2020, Teknologjia e informacionit – Teknikat e sigurisë – Kërkesa për organe ofruese të vlerësimit dhe certifikimit të sistemeve të menaxhimit të sigurisë së informacionit – Amendim 1.

ISO/IEC TS 27006-2:2021, Kërkesa për organe ofruese të vlerësimit dhe certifikimit të sistemeve të menaxhimit të sigurisë së informacionit – Pjesa 2: Sistemet e menaxhimit të informacionit për privatësinë.

ISO/IEC 17021-1:2015, Vlerësimi i konformitetit – Kërkesa për organe ofruese të vlerësimit dhe certifikimit të sistemeve të menaxhimit.

Politikat dhe rregulloret e zbatueshme të DPA-së.

Dokumentet e Detyrueshme IAF, sipas zbatueshmërisë.

## 5. FJALORI DHE SHKURTIME

Në këtë udhëzues është përdorur terminologjia nga
- Standardi ISO/IEC 17011:2017
- IAF Forum Ndërkombëtar i Akreditimit
- DPA Drejtoria e Përgjithshme e Akreditimit
- Standardet e posaçme të renditura më sipër.

## 6. PËRMBAJTJA

### 6.1. Të përgjithshme

ISO/IEC 27017 dhe ISO/IEC 27018 janë standarde ndërkombëtare, që ndihmojnë për të garantuar respektimin e parimeve të normativave për mbrojtjen e të dhënave (privacy) nga ana e ofruesve të platformave publike 'cloud', që duan t'i zbatojnë ato. Standardet u drejtohen posaçërisht atyre ofruesve të shërbimeve në 'cloud', të cilët përpunojnë të dhëna personale (PII - Personally Identifiable Information) dhe që veprojnë në cilësinë e Përpunuesit të të Dhënave (PII – Data Processor). Ato përcaktojnë linja udhëzues të bazuara në ISO/IEC 27002, duke marrë në konsideratë kërkesat normative për mbrojtjen e të dhënave personale, që mund të jenë të zbatueshme në kontekstin e tablosë se rreziqeve të sigurisë kibernetike të një furnitori të shërbimeve publike në 'cloud'. Standardet ISO/IEC 27017 e ISO/IEC 27018 janë linja udhëzuese dhe nuk janë të certifikueshme. Megjithatë, një certifikim ekzistues sipas ISO/IEC 27001, i lëshuar nga një organ vlerësimi i akreditуar, mund të plotësohet duke shtuar në të referencat sipas ISO/IEC 27017 e ISO/IEC 27018 për të dëshmuar aftësinë e furnitorit (Provider) për të siguruar mbrojtjen e të dhënave personale, bazuar në integrimin e këtyre standardeve me standardin ISO/IEC 27001.

Standardet janë ndërtuar mbi bazat e standardeve ISO/IEC 27001 e ISO/IEC 27002 në fushën e sigurisë së informacionit dhe përcaktojnë synimet e kontrollit, rregullave dhe procedurave për zbatimin e masave mbrojtëse për mbrojtjen e të dhënave personale (PII), në përputhje me parimet e privatësisë sipas ISO/IEC 29100 për furnitorët e shërbimeve në 'cloud'.

DPA nuk lëshon certifikatë akreditimi vetëm për standardet ISO/IEC 27017 dhe ISO/IEC 27018.

### 6.2. Rregulla për procesin e certifikimit

| | |
|---|---|
| Standardi i akreditimit | ISO/IEC 17021-1:2015, ISO/IEC 27006:2015, ISO/IEC 27006:2015 Amd.1:2020 |
| Standardi i certifikimit | ISO/IEC 27017 e ISO/IEC 27018 konsiderohen vetëm si shtesa ndaj standardit ISO/IEC 27001.<br>Standardi ISO/IEC 27017 mund të zbatohet si shtesë certifikimi më vete, pa ISO/IEC 27018.<br>Në rastet kur kjo shtesë do të përdoret edhe në lidhje me mbrojtjen e të dhënave personale, shtimi i standardit ISO/IEC 27017 duhet të kryhet bashkë me ISO/IEC 27018.<br>Nuk lejohet shtesa vetëm e standardit ISO/IEC 27018. |
| Kriteret per certifikim | Për të shtuar linjat udhëzuese ISO/IEC 27017 e ISO/IEC 27018 në një certifikim ISO/IEC 27001 ekzistues vlejnë këto kritere:<br><br>1. Shtesa mund të kryhet vetëm mbas një auditi në vend.<br><br>2. Nëse organizata ka tashmë një certifikim të vlefshëm ISO/IEC 27001 nga i njëjti Organ Vlerësimi dhe me një fushë certifikimi në përputhje me proceset e mbuluara nga standardet ISO/IEC 27017 e ISO/IEC 27018, auditi për zgjerimin do të kryhet vetëm me fazën e dytë në vend. Kohëzgjatja e auditit për secilën linjë udhëzuese do të jetë jo më pak se 30% e kohëzgjatjes së një auditi ricertifikimi ISO/IEC 27001, ku 1 ditë është kohëzgjatja minimale për selinë kryesore dhe 0,5 ditë për çdo seli tjetër të kampionuar, që përfshihet në shtesën për secilën linjë udhëzuese.<br><br>3. Nëse organizata ka një certifikim ISO/IEC 27001 nën akreditim EA-MLA, duhet fillimisht të kërkojë transferimin e certifikimit në OVK-në e akredituar nga DPA, dhe më pas mund të vijohet me certifikimin me zgjerim.<br><br>4. Nëse organizata nuk ka aktualisht një certifikim të vlefshëm të akredituar për ISO/IEC 27001, auditi do të kryhet sipas kritereve për një certifikim të ri për ISO/IEC 27001 dhe për ISO/IEC 27017 dhe ISO/IEC 27018 do të bëhet një rritje e kohës së auditit me jo më pak se 30% e kohës për një certifikim të parë ISO/IEC 27001. Kjo shtesë kryhet për secilën nga linjat udhëzuese (pra, dyfishi nëse është rasti për ISO/IEC 27017 dhe ISO/IEC 27018 së bashku), ku 1 ditë është kohëzgjatja minimale për selinë kryesore dhe 0,5 ditë për çdo seli tjetër të kampionuar. |

| | |
|---|---|
| | 5. Për mbikëqyrjet zbatohet gjithnjë shtesa e kohës së auditit me jo më pak se 0,5 ditë për selinë qendrore dhe 0,5 për çdo seli të kampionuar për secilën linjë udhëzuese.<br><br>6. Teknikat e auditimit duhet parashikojnë gjithnjë regjistrimin e evidencave të nevojshme për të garantuar zbatimin dhe plotë dhe shterues si të kërkesave të standardit ISO/IEC 27001, ashtu edhe të kërkesave shtesë nga standardet ISO/IEC 27017 e ISO/IEC 27018.<br><br>Para lëshimit të certifikimit duhet të jenë verifikuar të gjitha qendrat e të dhënave (data center), te të cilat janë vendosur serverat që menaxhojnë shërbimet në 'cloud'.<br><br>Në rast se organizata kërkon zgjerimin e certifikimit me të dyja standardet ISO/IEC 27017 dhe ISO/IEC 27018 njëri pas tjetrit, zgjerimi me standardin ISO/IEC 27017 duhet të jetë i pari. Nuk lejohet zgjerimi me standardin ISO/IEC 27018 pa mbështetjen e standardit ISO/IEC 27017.<br><br>Auditet e mbikëqyrjes dhe ricertifikimit:<br>Këto audite do të kryhen gjithnjë duke përfshirë të gjitha standardet si zgjerim i ISO/IEC 27001 dhe duke patur parasysh sa vijon:<br><br>Mbikëqyrja: një shtesë e kohës së auditit jo më pak se 30% e kohës së një mbikëqyrjeje për secilën linjë udhëzuese, dhe 0,5 ditë për çdo seli të kampionuar për secilën linjë udhëzuese.<br><br>Ricertifikimi: një shtesë e kohës së auditit jo më pak se 30% e kohës së një auditi ricertifikimi për secilën linjë udhëzuese dhe 0,5 ditë për çdo seli të kampionuar për secilën linjë udhëzuese. |
| Qendrat e të Dhënave në kontraktim (Data center in outsourcing) | Nëse qendrat e të dhënave (Data Center), që përdoren për veprimtaritë në 'cloud' janë në kontraktim të jashtëm te furnitorë që kanë certifikim të akredituar dhe të njohur në nivel EA-MLA për standardet ISO/IEC 27001, ISO/IEC 27017 dhe ISO/IEC 27018, mund të shmanget shtesa e kohës së auditit në këto seli. Në të gjitha rastet e tjera duhet të shtohet 0,5 ditë për çdo seli, që do të auditohet në vend.<br>Në rastet kur nuk është e mundur të kryhet një audit në vend (p.sh. te furnitorët e llojit Amazon e të ngjashëm), koha shtesë 0,5 ditë duhet të përdoret në selinë kryesore për auditimin e aspekteve kontraktuale dhe të kontrollit operativ me këta furnitorë. Kjo vlen vetëm në rastet, kur qendrat e të dhënave kanë certifikime TIER III ose TIER IV. |

| | |
|---|---|
| Kriteret e kompetencës për Ekipin Audites të OVK-së. | Ekipi audites duhet të zotërojë këto kompetenca:<br><br>● Auditor / Lead Auditor ISO/IEC 27001, me përvojë në vlerësimin e sistemeve ISO/IEC 27001 për jo më pak se 5 vjet. Preferohet të zotërojë certifikim personi profesional.<br>● Njohuri të standardeve ISO/IEC 27017 dhe/ose ISO/IEC 27018. |
| Kriteret e kompetencës për vendimmarrësin për certifikimin | Për të paktën një anëtar të grupit vendimmarrës, organi i vlerësimit të konformitetit duhet të dëshmojë:<br><br>● Kualifikimin si auditor ISO/IEC 27001.<br>● Njohuri të standardeve ISO/IEC 27017 dhe/ose ISO/IEC 27018. |
| Certifikata | Certifikata duhet t'i referohet gjithnjë standardit ISO/IEC 27001 dhe të citojë përdorimin e linjës udhëzuese ISO/IEC 27017 vetëm ose bashkë me ISO/IEC 27018 në zbatimin e saj. Në certifikatë duhet të jepen produktet, shërbimet, aplikacionet, apo proceset e mbuluara nga sistemi i certifikuar. |
| Dokumente IAF dhe EA | Vlejnë të gjitha dokumentet IAF dhe EA të zbatueshme për ISO/IEC 27001. |

### 6.3. Procesi i akreditimit

6.3.1. Kushte paraprake*:*

a) Organet certifikuese që aplikojnë për akreditim për skemën ISO/IEC 27017 e ISO/IEC 27018 duhet të jenë tashmë të akredituara nga DPA-ja sipas ISO 27001, ose
b) Organet certifikuese aplikojnë njëkohësisht për akreditim sipas ISO/IEC 27001 me shtesat për ISO/IEC 27017 dhe ISO/IEC 27018.

Organet certifikuese të akredituara për ISO/IEC 27001:2022 nga organizma akreditues të vendeve të tjera (pra, jo nga DPA) dhe që dëshirojnë të aplikojnë në DPA për zgjerim të programit të akreditimit për skemën ISO/IEC 27017:2015 dhe ISO/IEC 27018:2019, duhet fillimisht të kryejnë transferim të akreditimit për ISO/IEC 27001.

6.3.2. Vlerësimi i DPA për organet certifikuese që janë tashmë të akredituar nga DPA për skemën ISO/IEC 27001 dhe aplikojnë për zgjerim të programit të akreditimit kryhet si më poshtë:

| Veprimtaria akredituese | Mënyra e vlerësimit | Kohëzgjatja e vlerësimit |
|---|---|---|
| Zgjerim për skemën ISO/IEC 27017 dhe ISO/IEC 27018 | Vizitë në vend ku do të vlerësohet kompetenca e auditorëve dhe kryhet vlerësim vertikal.<br><br>Vlerësim me dëshmi (audit për certifikim fillestar). | Të paktën 1,5 ditë<br><br>Varet nga kohëzgjatja e vizitës audituese. |
| Mbikëqyrjet:<br>Gjatë ciklit të akreditimit do të kryhet të paktën një vizitë në zyrë dhe një vlerësim me dëshmi. | Vizitë në vend (vlerësim i kompetencës së auditorëve dhe vlerësim vertikal).<br><br>Vlerësim me dëshmi (audit për certifikim fillestar) | Të paktën 1 ditë<br><br>Varet nga kohëzgjatja e vizitës audituese |

Vlerësimi me dëshmi gjatë ciklit të akreditimit sipas skemës ISO/IEC 27017:2015 dhe ISO/IEC 27018:2019 mund të kryhet paralelisht me vlerësimin me dëshmi sipas ISO/IEC 27001:2022.

6.2.3 Vlerësimi i DPA skemën ISO/IEC 27017 dhe ISO/IEC 27018 për organet certifikuese që aplikojnë njëkohësisht për akreditim sipas ISO/IEC 27001 dhe ISO/IEC 27017 dhe ISO/IEC 27018 kryhet si më poshtë:

| Veprimtaria akredituese | Mënyra e vlerësimit | Kohëzgjatja e vlerësimit |
|---|---|---|
| Vlerësimi për akreditim fillestar për skemën ISO/IEC 27017 dhe ISO/IEC 27018 | Vizitë në vend ku do të vlerësohet kompetenca e auditorëve dhe kryhet vlerësim vertikal.<br><br>Vlerësim me dëshmi (audit për certifikim fillestar). | Të paktën 2 ditë<br><br>Varet nga kohëzgjatja e vizitës audituese. |

| | | |
|---|---|---|
| Mbikëqyrjet:<br>Gjatë ciklit të akreditimit do të kryhet të paktën një vizitë në zyrë dhe një vlerësim me dëshmi. | Vizitë në vend (vlerësim i kompetencës së auditorëve dhe vlerësim vertikal).<br><br>Vlerësim me dëshmi (audit për certifikim fillestar) | Të paktën 1 ditë<br><br>Varet nga kohëzgjatja e vizitës audituese |

Shënim: Nëse organi certifikues aplikon njëkohësisht për ISO/IEC 27001, atëherë kërkesat e parashtruara në këtë dokument u shtohen atyre në udhëzuesin përkatës për akreditimin sipas ISO/IEC 27001.
DPA mund të kryejë vlerësimin njëkohësisht për të dyja skemat.

Për organet me shumë vendndodhje: Për akreditim fillestare / zgjerim: të gjitha vendet ku kryhen aktivitetet kryesore do të vlerësohen me vizitë në vend. Gjatë ciklit të akreditimit: vendet ku kryhen aktivitetet kryesore do të vlerësohen të paktën një herë në dy vjet me vizitë në vend. Vendet e tjera do të vlerësohen të paktën një herë në ciklin e akreditimit me vizitë në vend.