Republika e Kosovës
Republika Kosova-Republic of Kosovo
Agjencia Shtetërore për Mbrojtjen e të Dhënave Personale
Državna Agencija za Zaštitu Ličnih Podataka
National Agency for Protection of Personal Data

RREGULLORE NR. 03/2015 MBI MASAT E SIGURISË GJATË PËRPUNIMIT TË TË DHËNAVE PERSONALE[1]

REGULATION NR. 03/2015 ON SECURITY MEASURES IN THE COURSE OF PERSONAL DATA PROCESSING[2]

PRAVILNIK BR. 03/2015 O MERAMA BEZBEDNOSTI TOKOM OBRADE LIČNIH PODATAKA[3]

[1] Rregullorja Nr. 03/2015 mbi masat e sigurisë gjatë përpunimit të të dhënave personale është miratuar në mbledhjen e 7 të Këshillit të Agjencisë, me Vendimin nr. 02/07 me datë : 24.04.2015

[2] Regulation No.03/2015 on security measures in the course of personal data processing is approved on the 7th session of Agency's Council with the deccission No. 02/07, dated 24.04.2015

[3] Pravilnik Br.03/2015 o merama bezbednosti tokom obrade licnih podataka odobreno je na 7 sednici Saveta Agencije, sa Odlukom br. 02/07 datuma: 24.04.2015

Në mbështetje të nenit 94 të Ligjit për Mbrojtjen e të Dhënave Personale Nr.03/L-172 (Gazeta Zyrtare e Republikës së Kosovës Nr. 70/31 maj 2010), neni 9 (paragrafi 9) i Rregullores së Punës së Agjencisë Shtetërore për Mbrojtjen e të Dhënave Personale Nr.20/2011 të datës 05.08.2011, Këshilli i Agjencisë Shtetërore për Mbrojtjen e të Dhënave Personale,	In support of Article 94 of the Law No. 03 / L-172 on Personal Data Protection (Official Gazette of the Republic of Kosovo, no. 70/31 May 2010), Article 9 (paragraph 9) of the Regulation on Procedure of the National Agency for Personal Data Protection No.20 / 2011 dated 05.08.2011, the Council of the National Agency for Personal Data Protection,	Na osnovu člana 94. Zakona o zaštiti ličnih podataka br. 03/L-172 (Službeni list Republike Kosovo br. 70/31 maj 2010. godine), član 9. (stav 9) Uredbe o radu Državne agencije za zaštitu ličnih podataka br. 20/2011 od dana 05.08.2011. godine, Savet Državne agencije za zaštitu ličnih podataka,
Miraton:	Adopts:	Usvaja:
RREGULLORE NR. 03/2015 MBI MASAT E SIGURISË GJATË PËRPUNIMIT TË TË DHËNAVE PERSONALE	**REGULATION NR. 03/2015 ON SECURITY MEASURES IN THE COURSE OF PERSONAL DATA PROCESSING**	**PRAVILNIK BR. 03/2015 O MERAMA BEZBEDNOSTI TOKOM OBRADE LIČNIH PODATAKA**
KAPITULLI I. DISPOZITAT E PËRGJITHSHME	**CHAPTER I. GENERAL PROVISIONS**	**POGLAVLJE I. OPŠTE ODREDBE**
Neni 1 Qëllimi	**Article 1 Purpose**	**Član 1 Svrha**
Qëllimi i kësaj Rregullore është përcaktimi i masave të përshtatshme organizative dhe teknike, logjiko-teknike për mbrojtjen e të dhënave personale dhe parandalimi i çfarëdo shkatërrimi të paqëllimshëm ose të qëllimshëm të paautorizuar, zbulimin, ndryshimin, parandalimin e qasjes dhe	The purpose of this Regulation is to determine the appropriate organizational and technical, logical-technical measures for the protection of personal data and prevent any accidental or unauthorized deliberate destruction, disclosure, modification, prevent unauthorized access and use of data	Svrha ovog Pravilnika je da utvrdi odgovarajuće organizacione i tehničke, logičke-tehničke mere za zaštitu ličnih podataka i sprečavanje slučajnog ili neovlašćenog namernog uništenja, objavljivanja, modifikacije, sprečavanje neovlašćenog pristupa i korišćenje podataka

përdorimit të paautorizuar të të dhënave apo humbjen e papritur ose të qëllimshme të tyre gjatë përpunimit të të dhënave personale nga organet publike dhe private.	and their accidental or deliberate loss in the course of processing of personal data by the public and private bodies.	ili njihovog slučajnog ili namernog gubitka u toku obrade ličnih podataka od strane javnih ili privatnih organa.
Neni 2 **Fushëveprimi**	**Article 2** **Scope**	**Član 2** **Delokrug**
1. Kjo Rregullore i referohet përpunimit manual dhe automatik.	1. This Regulation refers to the manual and automatic processing.	1. Ovaj Pravilnik se odnosi na ručnu i automatsku obradu.
2. Dispozitat lidhur me sigurinë e sistemeve të TIK-ut janë të detyrueshme vetëm për organet publike dhe private që përpunojnë të dhëna personale në mënyrë automatike.	2. The provisions concerning the security of ICT systems are mandatory only for public and private bodies that process personal data automatically.	2. Odredbe koje se odnose na bezbednost IKT sistema su obavezne samo za javne i privatne organe koji automatski obrađuju lične podatke.
3. Dispozitat që ndërlidhen me sigurinë fizike, mjedisore dhe të personelit janë të detyrueshme për organet që përpunojnë të dhëna personale në mënyrë manuale dhe automatike.	3. The provisions relating to physical, environmental and personnel security are mandatory for bodies that process personal data both manually automatically.	3. Odredbe koje se odnose na fizičku bezbednost, i bezbednost životne i sredine i osoblja su obavezne samo za organizavije koje ručno obrađuju lične podatke.
Neni 3 **Përkufizimet**	**Article 3** **Definitions**	**Član 3** **Definicije**
1. Shprehjet e përdorura në këtë Rregullore kanë kuptimin e mëposhtëm:	1. The terms used in this Regulation shall have the following meanings:	1. Izrazi upotrebljeni u ovom Pravilniku imaju sledeća značenja:
1.1. *Agjencia* nënkupton Agjencinë	1.1 *Agency* shall mean National Agency	1.1 *Agencija* podrazumeva Državnu

Shtetërore për Mbrojtjen e të Dhënave Personale e definuar me legjislacionin në fuqi;	for Personal Data Protection defined by the legislation in force;	Agenciju za Zaštitu Ličnih Podataka definisane prema zakonima na snati;
1.2. *Raporti i vlerësimit* nënkupton raportin mbi rezultatet e sigurisë së sistemit të dosjeve;	1.2 *Assessment report* shall mean the report on the outcome of the filing system security;	1.2 *Izveštaj o proceni* podrazumeva izveštaj o ishodu bezbednosti sistema za arhiviranje podataka;
1.3. *Organ publik dhe privat* nënkupton kontrolluesit dhe përpunuesit e të dhënave personale;	1.3 *Public and private body* shall mean the Controllers and Processers of personal data;	1.3 *Javni i privatni organi* podrazumeva kontrolore ili obrađivače ličnih podataka;
1.4. *Organet publike dhe private me Rrezikshmëri të Lartë* nënkupton Kontrolluesit ose Përpunuesit që përmbushin një nga kushtet e mëposhtme:	1.4 *High Risk public and private bodies* shall mean Controllers or Processors meeting one of the following conditions:	1.4 *Javni i privatni organi visokog rizika* podrazumeva kontrolore ili obrađivače koji ispunjavaju jedan od sledećih uslova:
1.4.1. përpunojnë të dhëna personale për më shumë se 100 subjekte të të dhënave gjatë një periudhe të pandërprerë 12 mujore;	1.4.1. processing of personal data relating to more than 100 data subjects during any consecutive 12 month period;	1.4.1 obrada ličnih podataka koja se odnosi na više od 100 nosilaca podataka tokom uzastopnog 12 mesečnog perioda;
1.4.2. përpunojnë kategori të veçanta të të dhënave personale, siç definohen në Nenin 2, paragrafi 1.16 të Ligjit për Mbrojtjen e të Dhënave Personale, të dhënat mbi vendndodhjen ose të dhënat mbi fëmijët ose të punësuarit në sistemet e dosjeve të një shkalle të gjerë;	1.4.2. processing of special categories of personal data as defined in Article 2, paragraph 1.16 of the Law on Data Protection, location data or data on children or employees in large scale filing systems;	1.4.2 obrada posebnih kategorija ličnih podataka kao što je navedeno u članu 2, tačka 1.16 Zakona o zaštiti ličnih podataka, podataka o lokaciji ili podataka o deci i zaposlenima u sistemima za arhiviranje podataka velikih razmera;
1.4.3. kryejnë profilizime, masa të	1.4.3. conduct profiling, measures	1.4.3 vrše profilisanje, mere koje

cilat mund të krijojnë efekte juridike në lidhje me individ ose në mënyrë të ngjashme prekin individ në masë të konsiderueshme;	which may produce legal effects concerning the individual or similarly significantly affect the individual;	mogu proizvesti pravno dejstvo u vezi pojedinca ili na sličan način znatno uticati na pojedinca;
1.4.4. përpunojnë të dhëna personale mbi ofrimin e kujdesit shëndetësor, hulumtimet epidemiologjike, ose hulumtime të sëmundjeve mendore ose infektive ku të dhënat përpunohen për marrjen e masave ose vendimeve në lidhje me individ të veçantë në një shkallë të gjerë;	1.4.4. processing of personal data for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;	1.4.4 obrada ličnih podataka za pružanje zdravstvene zaštite, epidemiološka istraživanja ili ankete mentalnih ili zaraznih bolesti, gde su podaci obrađeni za preduzimanje mera ili odluka o određenim pojedincima u velikim razmerama;
1.4.5. bëjnë monitorimin e automatizuar të zonave me qasje publike në një shkallë të gjerë;	1.4.5. automated monitoring of publicly accessible areas on a large scale;	1.4.5 automatizovana kontrola javno dostupnih mesta u velikim razmerama;
1.4.6. kryejnë veprime të tjera të përpunimit për të cilat kërkohet konsultimi i zyrtarit të mbrojtjes së të dhënave apo Agjencisë në pajtim me nenet 56 dhe 75 të Ligjit për Mbrojtjen e të Dhënave Personale;	1.4.6. other processing operations for which the consultation of the data protection officer or the Agency is required pursuant to Articles 56 and 75 of the Law on Data Protection;	1.4.6 vrše druge operacije obrađivanja za koje je potrebno konsultovanje službenika za zaštitu podataka ili Agencije na osnovu članova 56. i 75 Zakona o zaštiti ličnih podataka;
1.4.7. kur një shkelje mund të ndikojë negativisht në mbrojtjen e të dhënave personale, të privatësisë, të drejtave ose interesave legjitime të subjektit të të dhënave;	1.4.7. where a personal data breach would likely adversely affect the protection of the personal data, the privacy, the rights or the legitimate interests of the data subject;	1.4.7 kada bi kršenje verovatno negativno uticalo na zaštitu ličnih podataka, privatnosti, prava ili legitimne interese nosioca podataka;
1.4.8. aktivitetet kryesore të	1.4.8. the core activities of the	1.4.8 osnovne aktivnosti kontrolora

kontrolluesit ose përpunuesit përbëhen nga veprimet e përpunimit të cilat, për shkak të natyrës së tyre, fushëveprimit dhe/ose qëllimeve të tyre, kërkojnë monitorim të rregullt dhe sistematik të subjekteve të të dhënave;	controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects;	ili obrađivača se sastoje od postupaka obrade koji, zbog njihove prirode, obima i/ili potrebe, zahtevaju redovno i sistematsko praćenje nosioca podataka;
1.4.9. kur të dhënat personale janë të qasshme për një numër të personave numri i të cilëve nuk mund të jetë i kufizuar.	1.4.9. where personal data are made accessible to a number of persons which cannot reasonably be expected to be limited.	1.4.9 kada su lični podaci raspoloživi velikom broju osoba za koje se ne može očekivati da budu ograničeni.
1.5. Politika e Sigurisë së Informacionit ("PSI") nënkupton dokumentin përmes të cilit organi publik dhe privat i përpunimit të të dhënave iu komunikon punonjësve të vet dhe kontraktuesve (përpunuesve) si është ndërtuar, zbatohet dhe si funksion Sistemi i Menaxhimit të Sigurisë së Informacionit për mbrojtjen e të dhënave personale në një mënyrë të sigurt.	1.5 *Information Security Policy (PSI)* shall mean the document through which the public and private data processing body communicates to its employees and contractors (processors) how the Information Security Management System is constructed, implemented and operated for protecting personal data in a secure way.	1.5. *Politika bezbednosti informacija (PBI)* podrazumeva dokument kroz koji javni i privatni organ obrade podataka komunicira sa svojim zaposlenima i izvođačima (obrađivačima) kako je Sistem upravljanja bezbednošću informacija konstruisan, sproveden i upravljan za zaštitu ličnih podataka na siguran način.
1.6. *Organet publike dhe private të përpunimit të të dhënave me rrezikshmëri të ulët* nënkupton të gjithë kontrolluesit apo përpunuesit të cilët nuk bien në kategorinë e Rrezikshmërisë së Lartë.	1.6 *Low risk public and private data processing bodies* shall maean all those Controllers or Processors which do not fall into the High Risk category.	1.6. *Javni i privatni organi za obradu podataka niskog rizika* podrazumeva sve kontrolore ili obrađivače koji ne spadaju u kategoriju visokog rizika.
1.7. *TIK* nënkupton Teknologjinë e Informimit dhe Komunikimit.	1.7 *ICT* shall mean Information and Communications Technology	1.7. *ITK* podrazumeva Informaciona i Komunikaciona Tehnologija

1.8. *Personat përgjegjës* nënkupton të gjithë ata të cilëve iu lejohet qasje në të dhënat personale nga ana e organit publik dhe privat të përpunimit të të dhënave. Kategoritë kryesore të personave të obliguar për mbrojtjen e të dhënave personale janë:	1.8 *Persons in charge* shall mean all those who are granted with an access to personal data by public and private data processing boddies. The main categories of persons, obliged to safeguard the personal data are:	1.8 *Zadužene Osobe* podrazumeva sve one kojima se odobrava pristup ličnim podacima od strane javnih i privatnih rgana za obradu podataka. Glavne kategorije lica, koja su u obavezi da štite lične podatke su:
1.8.1. Administratorët e sistemeve të Teknologjisë së Informimit dhe Komunikimit dhe të sigurisë së tyre, të cilët i nënshtrohen këtij obligimi kur organi publik dhe privat ka një sistem të TIK-ut të themeluar me qëllim të procesimit të të dhënave personale.	1.8.1. Administrators of Information and Communication Technology systems and of their security, who are subjected to this obligation when a public or private body has an ICT system established to for purpose of personal data processing.	1.8.1 Administratori sistema informaciono-komunikacionih tehnologija i njihove bezbednosti, koji podležu ovoj obavezi kada javni i privatni organ poseduje jedan IKT sistem uspostavljen za tu namenu.
1.8.2. Operatorët e të dhënave personale (punëtorët, kontraktuesit, etj) që përpunojnë të dhëna personale duke përdorur mjetet e TIK-ut, me qëllim të përmbushjes së detyrave të tyre, gjatë punës në organin publik dhe privat për përpunimin e të dhënave personale.	1.8.2. Personal data operators (employees, contractors, etc.) which process personal data using ICT means for the purpose of fulfilling their tasks while working for the public and private personal data processing body.	1.8.2 Operatori ličnih podataka (zaposleni, izvođači, itd) koji obrađuju lične podatke koristeći IKT sredstva radi ispunjavanja svojih zadataka radeći za javni i privatni organ za obradu ličnih podataka.
1.8.3. Të gjithë personat e tjerë të caktuar nga organi publik dhe privat i përpunimit të të dhënave për të përpunuar të dhëna personale në mënyrë manuale.	1.8.3. All other persons assigned by the public and private data processing body to process personal data manually.	1.8.3 Sva ostala određena od strane javnog i privatnog organa za obradu podataka da ručno obrađuju podatke.

1.9. *Analiza e Rreziqeve* nënkupton analizën e rrezikshmërisë, vlerësimit dhe trajtimit ashtu si është definuar në nenin 6 të kësaj Rregullore.	1.9. *Risk Analysis* means risk analysis, assessment and treatment as defined in Article 6 of this Regulation.	1.9 *Pojednostavljena analiza rizika* podrazumeva analizu rizika kako je definisana u članu 6. ovog Pravilnika.
1.10. *SMSI* nënkupton Sistemi i Menaxhimit të Sigurisë së Informacionit.	1.10. *ISMS* mean Information Security Management System.	1.10 *SUBI* podrazumeva Sistem upravljanja bezbednosti informacija.
1.11. *Cloud Computing* nënkupton një model për të mundësuar qasje të gjithëpranishme, të përshtatshme, në rrjet në bazë të kërkesës, në grupin e përbashkët të burimeve të konfigurueshme kompjuterike (p.sh. rrjetat, serverët, depove të të dhënave, aplikacioneve dhe shërbimeve) që mund të ofrohen dhe lëshohen me shpejtësi me përpjekje minimale të menaxhimit ose bashkëveprimit të ofruesit të shërbimit.	1.11. *Cloud Computing* means a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.	1.11 *Cloud Computing* podrazumeva model za omogućavanje sveprisutnog, praktičnog, pristupa mreži na zahtev, zajedničkoj grupi podesivih računarskih resursa (na primer, mreže, serveri, skladištenje, aplikacije i usluge) koje se mogu brzo pružiti i puštati uz minimalni upravljački napor ili interakciju provajdera usluga.
1.12. *Shkelje e të dhënave personale* nënkupton një shkelje të sigurisë që çon në shkatërrim aksidental apo të paligjshëm, humbje, ndryshim, zbulim të paautorizuar apo qasje në të dhënat personale të përpunuara	1.12. *Personal data breach* means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data processed.	1.12 *Kršenje ličnih podataka* podrazumeva kršenje bezbednosti koje vodi do slučajnog ili nezakonitog uništavanja, gubitka, menjanja, neovlašćeno otkrivanje, ili pristup obrađenim ličnim podacima
2. Termet e përdorura në këtë Rregullore, që nuk janë përkufizuar në paragrafin 1 të këtij neni, do të kenë kuptimin e përkufizuar me Ligjin për Mbrojtjen e të Dhënave	2. The terms used in this Regulation which are not defined in paragraph 1 of this Article shall have the meaning as defined by the Law on Personal Data Protection.	2. Izrazi upotrebljeni u ovom Pravilniku koji nisu definisani u stavu 1. ovog člana imaju značenje kao što je utvrđeno Zakonom o zaštiti ličnih podataka.

Personale. **Neni 4** **Zbatimi për organet publike dhe private me Rrezikshmëri të Lartë dhe me Rrezikshmëri të Ulët** 1. Kapitulli II i kësaj Rregullore zbatohet për organet publike dhe private të përpunimit të të dhënave me rrezikshmëri të Ulët dhe të Lartë. Kapitulli III i këtij Udhëzimi Administrativ do të zbatohet vetëm nga organet publike dhe private të përpunimit të të dhënave me rrezikshmëri të Lartë. **KAPITULLI II** **KËRKESAT E PËRGJITHSHME PËR ORGANET PUBLIKE DHE PRIVATE TË PËRPUNIMIT TË TË DHËNAVE ME RREZIKSHMËRI TË ULËT DHE TË LARTË** **Neni 5** **Dispozitat themelore mbi sigurinë** 1. Organet publike dhe private janë përgjegjëse për sigurinë e të dhënave personale duke i mbrojtur ato nga dëmtimet aksidentale apo të paligjshme, nga	**Article 4** **Application to High-Risk and Low-Risk public and private bodies** 1. Chapter II of this Regulation is applied for Low risk public and private data processing bodies as well as for High risk. Chapter III of this Regulation shall be applied only by public and private High risk data processing bodies. **CHAPTER II** **GENERAL REQUIREMENTS FOR LOW- AND HIGH-RISK PUBLIC AND PRIVATE DATA PROCESSING BODIES** **Article 5** **Basic security provisions** 1. The public and private bodies are responsible for the security of personal data by protecting them against accidental or unlawful damage or destruction, accidental	**Član 4.** **Primena na javne i privatne organe visokog i niskog rizika** 1. Poglavlje II ovog Pravilnika se primenjuje na javne i privatne organe za obradu podataka niskog i visokog rizika. Poglavlje III ovog Pravilnika će se primeniti samo od strane javnih i privatnih organa za obradu podataka visokog rizika. **POGLAVLJE II** **OPŠTI USLOVI ZA JAVNE I PRIVATNE ORGANE ZA OBRADU PODATAKA NISKOG I VISOKOG RIZIKA** **Član 5** **Osnovne odredbe bezbednosti** 1. Javni i privatni organi su odgovorni za bezbednost ličnih podataka štiteći ih od slučajnog ili nezakonitog oštećenja ili uništenja, slučajnog gubitka, menjanja,

shkatërrimi ose humbja aksidentale, ndryshimi, qasja e paautorizuar dhe vënia e tyre në dispozicion të personave të paautorizuar si dhe nga çdo formë tjetër e paautorizuar e përpunimit.	loss, alteration, unauthorized access and making them available to unauthorized persons, and against any other unauthorized form of processing.	neovlašćenog pristupa i činećи ih nedostupnim neovlašćenim licima, i protiv bilo kog drugog neovlašćenog oblika obrade.
2. Me qëllim të zbatimit të paragrafit 1 më lartë, organet publike dhe private ndërmarrin masat e duhura teknike, organizative dhe të lidhura me personelin, të përshtatshme për mënyrën përkatëse të përpunimit, duke marrë parasysh, mbi të gjitha:	2. In order to implement paragraph 1 above, public and private bodies take adequate technical, organizational and personnel related measures being appropriate to the particular processing manner, while they shall take into account, above all:	2. U cilju sprovođenja tačke 1, javni i privatni organi preduzimaju adekvatne tehničke, organizacione i kadrovske mere koje su adekvatne za određeni način obrade, uzimajući u obzir, pre svega:
2.1. Mjetet dhe masat teknike ekzistuese, veçanërisht ato të përcaktuara nga ligjet specifike sektoriale, nëse janë të zbatueshme;	2.1. The existing technical means and measures, especially those instructed by the sector specific laws, if applicable.	2.1. Postojeća tehnička sredstva i mere, posebno one naložene specifičnim sektorskim zakonima, ako su primenljive.
2.2. Nivelin e rrezikut potencial për funksionimin e qëndrueshëm dhe të sigurt të sistemit të përpunimit të të dhënave personale. Në veçanti duhet trajtuar ato rreziqe të cilat rezultojnë në cenueshmëri që mund të përfundojnë me rreziqe të materializuara në:	2.2. The level of potential threats to the stable and secure functioning of the personal data processing system. Especially those threats shall be addressed which lead to vulnerabilities which may end up with materialised risks to:	2.2. Nivo potencijalnog rizika za stabilno i sigurno funkcionisanje sistema za obradu ličnih podataka. Posebno moraju da se reše ti rizicikoji dovode do ranjivosti i koji mogu završiti u materijalizovanim rizicima u:
2.2.1. Konfidencialitetin, integritetin dhe disponueshmërinë e të dhënave dhe sistemin e përpunimit të tyre;	2.2.1. Confidentiality, integrity and availability of the data and its processing system;	2.2.1. Poverljivost, integritet i dostupnost podataka i njegovog sistema za obradu;

2.2.2. Përgjegjësinë e sistemit të përpunimit të tyre.	2.2.2. Accountability of its processing system.	2.2.2. Odgovornost njegovog sistema za obradu.
2.3. Organet publike dhe private duhet të jenë në gjendje të dëshmojnë nivelin dhe përmbajtjen e masave të ndërlidhura teknike, organizative dhe të personelit, të ndërmarra në bazë të kësaj Rregullore. Këto masa duhet të dokumentohen dhe ky dokumentim duhet të jetë në dispozicion të Agjencisë, sipas kërkesës së saj.	2.3. The public and private bodies shall be able to prove the level and content of the technical, organizational and personnel related measures taken according to this Regulation. These measures shall be documented, and this documentation is to be made available to the Agency on its request.	2.3. Javni i privatni organi moraju biti u stanju da dokažu nivo i sadržaj tehničkih, organizacionih i kadrovskih mera koje su preduzete u skladu sa ovim Administrativnim uputstvom. Ove mere da se dokumentiraju, i ovo dokumentiranje treba da bude na raspolaganju Agenciji na njen zahtev.
3. Organi publik dhe privat duhet të autorizojë, me shkrim, një person përgjegjës për mbikëqyrjen e sigurisë së të dhënave personale. Nëse një zyrtar për mbrojtjen e të dhënave personale është i caktuar në pajtim me Ligjin për Mbrojtjen e të Dhënave Personale dhe Udhëzimin Administrativ nr. 01/2011, ky zyrtar mund të autorizohet për të mbrojtur sigurinë e të dhënave personale në përputhje me këtë Rregullore.	3. The public and private body shall authorize, in writing, a person in charge of supervision of personal data security. If a personal data protection official is appointed pursuant to Law on Personal Data Protection and Administrative Instruction No. 01/2011, this official can be authorized to safeguard personal data security according to this Regulation.	3. Javni i privatni organ Subjekat za obradu podataka može da ovlasti, u pisanoj formi, osobu zaduženu za nadzor očuvanja sigurnosti ličnih podataka. Ako se imenuje službenik za zaštitu ličnih podataka na osnovu Zakona o zaštiti ličnih podataka i Administrativnom uputstvu br. 01/2011, ovaj službenik će biti ovlašćen da štiti bezbednost ličnih podataka.
Neni 6 **Analiza dhe vlerësimi i thjeshtësuar i rreziqeve**	**Article 6** **Risks Analysis and Assessment**	**Član 6** **Pojednostavljenje Analize i Procene rizika**
1. Çdo organ publik dhe privat i përpunimit të të dhënave harton Analizën e Rreziqeve ku identifikohen kërcënimet që prekin pjesë	1. Each public and private data procesing body drafts Risks Analysis which identifies the threats affecting individual parts of the	1. Svaki javni i privatni organ obrade podataka izrađuje pojednostavljenu analizu rizika kojom se identifikuju pretnje koje

individuale të sistemit të dosjeve, të cilat mund të shpijnë në cenueshmëri dhe mund të materializohen me shkelje të sigurisë së përpunimit të të dhënave.	filing system, which can lead to vulnerabilities and able to materialise as a security breach of data processing.	utiču na pojedinačne delove sistema arhiviranja, koje mogu dovesti do ranjivosti koja je u stanju da se materijalizuje kao povreda bezbednosti obrade podataka.
2. Rezultati i analizës së rreziqeve duhet të përmbajë:	2. The outcome of risks analysis shall contain:	2. Ishod pojednostvljene analize rizika treba da sadrži:
2.1. Listën e kërcënimeve dhe cenueshmërisë të cilat mund të rrezikojnë konfidencialitetin, integritetin dhe disponueshmërinë e të dhënave personale që përpunohen, dhe sistemin e përdorur për atë përpunim.	2.1. List of threats and vulnerabilities which can endanger the confidentiality, integrity and availability of personal data being processed, and of the system used for such processing.	2.1 Spisak pretnji i ranjivosti koje mogu ugroziti poverljivost, integritet i dostupnost ličnih podataka koji se obrađuju, i sistem koji se koristi za takvu obradu.
2.2. Listën e kërcënimeve dhe cenueshmërisë që mund të shkaktojnë dëmtim të vërtetë të të dhënave dhe sistemit të përpunimit të tyre, përfshirë vlerësimin e kërcënimeve dhe cënueshmërisë që me gjasë mund të ndodhin dhe koston e masave për parandalimin e paraqitjes së tyre.	2.2. The list of threats and vulnerability that can cause real damage to data and their processing system, including the assessment of threats and vulnerabilities that are likely to occur and the cost of measures to prevent their appearance.	2.2 Spisak pretnji i ranjivosti koje mogu izazvati stvarno oštećenje podataka i sistema njihove obrade, uključujući procenu pretnji i ranjivosti koje se eventualno mogu pojaviti i troškove za mere sprečavanja njihovog pojavlivanja.
2.3. Listën e mjeteve dhe masave përkatëse që do të aplikohen për të zbutur ndikimin e këtyre rreziqeve të identifikuara duke përfshirë masat teknike të sigurisë dhe masat organizative të sigurisë – në formë të udhëzimeve dhe procedurave.	2.3. List of means and appropriate measures to be applied to mitigate the impact of these risks identified including technical security measures and organisational security measures – in form of instructions and procedures.	2.3. Spisak adekvatnih pomagala i mera koje će se primeniti za ublažavanje ovih identifikovanih rizika uključujući ,tehničke mere bezbednosti i organizacione mere bezbednosti - uputstva i postupci.

2.4. Listën e rreziqeve të pranuara (rreziqet e mbetura) me arsyetimin se pse janë pranuar, vetëm duke u zvogëluar (parandaluar) në një mënyrë të kufizuar.	2.4. List of accepted risks (residual risks) with an explanation why they are actually accepted thus being mitigated (prevented from) in a limited way only.	2.4. Spisak prihvaćenih rizika (preostalih rizika) sa obrazloženjem zašto su oni prihvaćeni.
3. Organi publik dhe privat është i lirë të zgjedhë se si këto procedura do të dokumentohen, mirëmbahen dhe t'u komunikohen personave të cilët përpunojnë të dhënat.	3. The public and private body is free to choose how these procedures will be documented, maintained and communicated to persons who process data.	3. Javni i privatni organ je slobodan da izabere kako će ove procedure biti dokumentovane, održava i saopštava licima koja obrađuju podatke.
4. Kjo analizë e rreziqeve duhet të bëhet në mënyrë periodike, së paku një herë në vit, dhe duhet të dokumentohet në gjuhën që zakonisht përdoret në praktikën e veprimtarisë të organit publik dhe privat.	4. This risk analysis is to be carried out periodically, minimum once a year, and documented using the language commonly applied to the particular public and private bodies business practice.	4. Analiza rizika treba da se vrši na periodičan način, najmanje jednom godišnje, i dokumentuje upotrebom jezika koji se obično primenjuje u poslovnoj praksi javnog i privatnog organa.
5. Organi publik dhe privat me rrezikshëmri të ulët mund të hartojë dhe të dokumentojë këtë analizë të rrezikut dhe vlerësimin e saj në një formë të thjeshtëzuar, duke përdorur praktikën e veprimtarisë.	5. Low-risks private and public bodies may carry out and document such a risk analysis and assessment in a simplified form, using their everyday business practice language.	5. Privatni i javni organi niskog rizika može obaviti i dokumentovati takvu analizu i procenu rizika u pojednostavljenom obliku, koristeći jezik svoje svakodnevne poslovne prakse.
Neni 7 **Aranzhimet Minimale për Vazhdimësinë e Veprimtarisë**	**Article 7** **Minimal Business Continuity Arrangements**	**Član 7** **Minimalne radnje za kontinuitet poslovanja**
1. Organi publik dhe privat duhet të përgatit veteveten për ngjarje të paparashikuara që mund të rrezikojnë	1. The public and private body shall prepare itself for unpredicted events which may endangering its very existence due to	1. Javni i privatni organ će se pripremiti za nepredviđene događaje koji mogu ugrožavati njegov opstanak zbog

ekzistencën e tij për shkak të mungesës së duhur dhe të sigurt të përpunimit të të dhënave në përputhje me formën që përdoret në praktikën e përditshme të veprimtarisë.	lack of proper and secure data processing in accordance with the form is used for its everyday business practice.	nedostatka pravilne i bezbedne obrade podataka u skladu sa oblikom koji se koristi u svakodnevnoj poslovnoj praksi.
2. Organi publik dhe privat duhet të përcaktojë dispozita që do të përdoren në situata të jashtëzakonshme dhe katastrofike, në mënyrë që të mundësojë vazhdimësinë e veprimtarisë.	2. Public and private body it shall describe provisions to be used in extraordinary and catastrophic situations, in order to allow for business continuity.	2. Javni i privatni organ treba da odredi odredbe koje će se koristiti u vanrednim i situacijama katastrofa, kako bi se omogućio kontinuitet poslovanja.
3. Dispozitat e parapara sipas paragrafit 2 të këtij Neni duhet t'i referohen vetëm situatave të rralla që mund të çojnë në ndryshime të rëndësishme të paplanifikuara në mënyrën se si kryhet përpunimi, veçanërisht për ato që rezultojnë nga mungesa e shërbimeve të nevojshme për përpunimin e të dhënave në një mënyrë të qëndrueshme dhe të sigurt, si dhe përshkruajnë se si përpunimi i të dhënave do të kthehet përsëri në kushtet e gjendjes normale.	3. The provisions under paragraph 2 of this Article shall refer only to the very seldom situations which may lead to significant unplanned changes in the way the processing is conducted, especially to those resulting from the lack of services required to process data in a stable and secure way, as well to describe how the data processing will return to normal conditions.	3. Predviđene odredbe prema tački 2 ovog člana treba da se: odnose na vrlo retke situacije koje mogu dovesti do značajnih neplaniranih promena u načinu na koji se obrada vodi, posebno na one koje su rezultat nedostatka usluga potrebnih za obradu podataka na stabilan i siguran način, kao i opisuju kako će se obrada podataka ponovo vratiti u normalnom stanju.
4. Organi Publik dhe Privat në funksion të implementimit të këtij neni mund të marrë vendim të:	4. The Public and Private body in order to implement this article may take decision to:	4. Javni I privatni organ u funkciji sprovođenja ovog člana može da odluči da se:
4.1. Ndalohet tërësisht përpunimi;	4.1. Stop the processing altogether;	4.1. Zaustavi potpuno obrada
4.2. Vazhdohet në një formë të kufizuar	4.2. Continue it in a limited secure form;	4.2. Nastavi na jedan ograničen i siguran

dhe të sigurt; 4.3. Vendosë disa mjete alternative teknike të përpunimit (p.sh kalimi nga përpunimi automatik në përpunim manual) dhe shërbime alternative të përpunimit të të dhënave.	4.3. Deploy some alternative technical processing means (e.g. by switching from automatic to manual processing), and alternative data processing services.	oblik 4.3. Razvije neke alternativne tehničke načine za obradu (npr. prelaskom sa autamatskog na ručnu obradu), i alternativne usluge obrade podataka.
Neni 8 **Standardet minimale të sigurisë fizike dhe mjedisore** 1. Sistemet e përpunimit të informacionit, programet ose pajisjet e TIK-ut ku mbahen bazat e të dhënave mund të qasen vetëm nga personat e autorizuar. 2. Kopjet rezervë të të dhënave "backup" duhet të bëhen me një shpejtësi që korrespondon me shpejtësinë e ndryshimit të të dhënave. Këto kopje duhet: 2.1. të enkriptohen 2.2. një kopje duhet të vendoset në një vend tjetër fizikisht larg nga vendi i përpunimit, në mjedise të sigurta të cilat nuk i ekspozohen rreziqeve si: zjarri, tërmeti, përmbytjet apo vjedhja.	**Article 8** **Minimal physical and environmental security standards** 1. The information processing systems, programs or ICT equipment where a databases are kept, are to be accessed by authorised persons only. 2. Backup of data is to be made with a frequency corresponding to how often the data is changed. These copies are: 2.1. to be encrypted 2.2. One copy shall be placed in another distant physical location, at safe premises which are not exposed to the risks such as fire, earthquake, flood or theft.	**Član 8** **Minimalni standardi fizičke bezbednosni i bezbednosti životne sredine** 1. Sistemima i programima za obrađivanje informacija, ili IKT opremi, gde se baza podataka održava, mogu pristupiti samo ovlašćena lica. 2. Rezervne kopije podataka "backup" vrše se brzinom koja odgovara brzini kojom se menjaju podaci. Ove kopije treba: 2.1. da se enkriptuju 2.2. jedna kopija se čuva na drugoj udaljenoj fizičkoj lokaciji, na sigurnim prostorijama koje nisu izložene istim rizicima kao što su požari, zemljotres, poplave ili krađe.

3. Qasja fizike në të dhënat personale dhe pajisjet e TIK-ut për përpunimin e tyre i jepet vetëm personave të autorizuar dhe informatat mbi qasjen (regjistrat) duhet të mbahen në një vend dhe formë të sigurt, në dispozicion vetëm për ata që iu është lejuar qasja, ku periudha e ruajtjes së regjistrave të tillë është së paku një vit.	3. Physical access of personal to data and its ICT processing equipment is granted to authorised persons only and records of such access (logs) are to be kept in a secure place and form, available only for those who had been granted such an access, whereas the retention periods for of such logs are minimum one year.	3. Fizički pristup ličnim podacima i IKT opremi za njihovu obradu se dodeljuje samo ovlašćenim licima i evidencije o takvim pristupima (zapisnici) treba da se čuvaju na sigurnom mestu i obliku, na raspolaganju samo onima kojima je takav pristup bio dozvoljen, gde period zadržavanje takvih zapisnika je najmanje godinu dana.
4. Të gjitha mediumet fizike që përmbajnë të dhëna personale duhet të shkatërrohen pas arritjes së qëllimit për të cilin janë përdorur, në veçanti:	4. All physical media containing personal data are to be destroyed when they have fulfilled the purpose for which they were used, in particular:	4. Sve fizičke medijume koji sadrže lične podatke treba uništiti, kada su ispunili svrhu za koju su korišćeni, naročito:
4.1. Shkresat, përfshirë fotokopjet, fotografitë;	4.1. Printouts, including photocopies, photographs;	4.1. Ispise uključujući fotokopije, fotografije;
4.2. Bartësit tjerë të të dhënave, si: CD ROM, DVD ROM, shiriti për incizim të kopjes rezervë "backup";	4.2. Other data carriers, such as CD ROM, DVD ROM, backup recording tape;	4.2.Drugi nosioci podataka, kao što su CD ROM, DVD ROM, arhivska magnetna traka "backup"
4.3. Formularët e plotësuar dhe regjistrat në kopje fizike.	4.3. Filled forms, and paper registers.	4.3.Popunjeni formulari i registri u fizičkim kopijama.
5. Në rastin e pajisjeve portative elektronike dhe mjeteve tjera me memorie, të përdorura për të ruajtur të dhënat personale, shkatërrimi i të dhënave bëhet duke hequr përmbajtjen e informacionit në një mënyrë që rikthimi i të dhënave nuk	5. In case of portable electronic equipment and other memory tools, used to store personal data, the data destruction is to be made by removing their information content in a manner that restoring it is no more possible using technical means	5. U slučaju automatske prenosive opreme i drugih memorijskih sredstava, korišćenih za čuvanje ličnih podataka, uništavanje podataka će se vršiti ukidanjem njihovog informativnog sadržaja na način da obnavljanje više nije moguće korišćenjem

është i mundur me mjetet teknike në dispozicion në treg. 6. Një " Politikë e mbajtjes së tavolinave të pastërta"" duhet të zbatohet në rast të kontraktimit të ofruesve të shërbimeve të cilët janë të lejuar të hyjnë në lokalet e organit publik dhe privat në mungesë të personelit të vetë përgjegjës për sigurinë e përpunimit të të dhënave, veçanërisht në rastin e shërbimeve të tilla si: pastrimi i zyrave dhe mirëmbajtja, rojet e sigurisë, asistenca teknike dhe shërbime tjera. **Neni 9** **Standardet minimale të sigurisë logjike të pajisjeve të TIK-ut** 1. Nëse përdoren pajisjet personale të TIK-ut në përpunimin e të dhënave personale: 1.1. Ligjshmëria e përdorimit të të gjitha programeve që aplikohen në përpunimin e të dhënave personale duhet të kontrollohen rregullisht. Përditësimet e sigurisë duhet të aktivizohen. 1.2. Masat e sigurisë duhet të vendosen për:	available on the market. 6. A *"clean desk policy"* is to be implemented in case of contracting service providers which are allowed to enter premises of public and private bodies on absence of own personnel responsible for security of data processing, in particular such services as office cleaning and maintenance, security guards, technical assistance and other services. **Article 9** **ICT equipment logical security minimum standards** 1. If own ICT equipment is deployed to processing of personal data: 1.1. Legality of use of all software applied to personal data processing shall be regularly checked. Security updates shall be activated. 1.2. Security measures shall be in place to:	tehničkih sredstava dostupnih na tržištu. 6. Jedna *„Politika čistog stola"* treba da se realizuje u slučaju ugovaranja provajdera usluga kojima je dozvoljen ulazak u prostorije javnog I privatnog organa u odsustvu sopstvenih kadrova odgovornih za bezbednost obrade podataka, posebno takvih usluga kao što su čišćenje i održavanje kancelarije, obezbeđenje, tehnička pomoć i ostale usluge. **Član 9** **Minimalni standardi logičke bezbednosti ITK opreme** 1. Ako se upotrebljava lična IKT oprema za obradu ličnih podataka: 1.1. Zakonitost korišćenja svih softvera primenjenih na obradu ličnih podataka se redovno proverava, Ažurniranje bezbednosti treba da se aktivira. 1.2. Mere bezbednosti će biti na snazi:

1.2.1. Dhënien e të drejtës për qasje individuale për t'i mundësuar çdo përdoruesi të punojë vetëm në llogarinë e tij personale, duke përdorur së paku mjetet unike të autentikimit, të tilla si "emri i përdoruesit" dhe "fjalëkalimi", periodikisht të ndryshueshme dhe po ashtu rekomandohen të përdoren mjete të fuqishme të autorizimit dhe identifikimit.	1.2.1. Individual access rights shall be granted to enable each user to work on his personal account only, using unique authentication means, such as "user name" and periodically changeable "password" as a minimum, and it is also recomended to use stronger authorisation and identification means.	1.2.1. Individualna prava na pristup se odobravaju da omoguće svakom korisniku da radi samo na njegovom ličnom nalogu, koristeći jedinstvena sredstva potvrde identiteta, kao što su periodično promenljivo "korisničko ime" i "lozinka" i takođe se preporučuju jača sredstva za ovlašćenje i proveru identiteta.
1.2.2. Mundësia e përdorimit të mediumeve portative, duhet të kufizohet vetëm në rastet kur kjo është absolutisht e nevojshme, dhe duhet të aplikohet monitorimi i përdorimit të mediumeve të tilla.	1.2.2. The possibility to attach any external media shall be limited to the cases when it is absolutely required, and monitoring of uses of such media shall be implemented.	1.2.2. Mogućnost korišćenja prenosivih medijuma će biti ograničena na slučajeve kada je apsolutno potrebno, i sprovodiće se praćenje upotrebe pomenutih medijuma.
1.2.3. Përdoruesit duhet të njoftohen se duhet të enkriptohen të gjitha mediumet e tilla në rast të largimit të tyre nga objektet e përpunimit të dhënave.	1.2.3. Users shall be informed that it is required to encrypt all such media in case they may leave the premises.	1.2.3. Korisnici će biti obavešteni da je potrebno enkriptirati sve takve medijume u slučaju napuštanja zgrade obrade podataka.
2. Në rast të kontraktimit të shërbimit për mirëmbajtje të pajisjeve të TIK-ut për përpunimin e të dhënave personale:	2. In case of using an external service contracted to maintain ICT equipment for processing personal data:	2. U slučaju korišćenja spoljne službe ugovorene za održavanje IKT opreme za obradu ličnih podataka:
2.1. Përdoruesit e palës së kontraktuar të cilët mund të kenë qasje në të dhënat	2.1. Users of the contracted party who	2.1. Korisnici ugovorene stranke koja može imati pristup ličnim podacima u

personale gjatë kryerjes së detyrave të tyre, duhet të trajtohen si personel i brendshëm në aspektin e sigurisë së të dhënave. 2.1.1. Dispozitat përkatëse mbi sigurinë e përpunimit të të dhënave personale duhet të përfshihen në kontratë me palën e kontraktuar, përveç nëse pala e tretë nuk do të ketë qasje në të dhëna personale gjatë ekzekutimit të kontratës. 3. Në rast të përdorimit të një shërbimi të jashtëm me qira të pajisjeve të TIK-ut për përpunimin e të dhënave personale: 3.1. Duhet të përdoren komponentët e sigurisë të rekomanduar dhe të aktivizuar nga ofruesi i shërbimit. 3.2. Pas përfundimit të kontratës së qirasë duhet të hiqen të gjitha të dhënat personale nga sistemet dhe pajisjet që do t'i kthehen pronarit, në atë mënyrë që rikthimi i të dhënave në ato pajisje dhe sismte të është i pamundur.".	may have access to personal data while carrying out their duties shall be treated as own personnel in terms of data security. 2.1.1. The corresponding personal data processing security clauses shall be included in the contract with such a party, unless the third party will be never able to access the personal data during the contract's execution. 3. In case of using an external service renting ICT equipment for personal data processing: 3.1. Security components advised and activated by the service provider shall be used. 3.2. Upon the termination of the rental contract, all personal data shall be removed from the systems and the equipment to be returned to the owner, so as restoration of previous information on them is no more possible.	obavljanju svojih dužnosti će se tretirati kao sopstveno osoblje u pogledu bezbednosti podataka. 2.1.1. Odgovarajuće bezbednosne klauzule za obradu ličnih podataka moraju biti uključene u ugovor sa takvim strankama, osim ako treća strana nikad neće moći da pristupi ličnim podacima tokom izvršenja ugovora. 3. U slučaju korišćenja spoljne službe iznajmljenom IKT opremome za obradu ličnih podataka: 3.1. Treba da se koriste bezbednosne komponente preporučene i aktivirane od strane provajdera usluge. 3.2. Nakon završetka ugovora iznajmlivanja, svi lični podaci će biti uklonjeni iz sistema i opreme koja se vraća vlasniku, na način na koji obnavljanje prethodnih informacija je nemoguće.

Neni 10 **Standardet minimale të sigurisë gjatë qasjes në rrjetet publike sic është rasti në Internet**	Article 10 **Minimum security standards when accessing public networks such as Internet**	Neni 10 **Minimalni standardi za bezbednost prilikom pristupa javnim mrežama**
1. Në rast të përdorimit të qasjes në rrjetet publike, standardet minimale që duhet të implementohen përfshijnë:	1.In case of using public networks access, minimum standards that shall be implemented include:	1. U slučaju upotrebe pristupa na javnim mrežama, minimalni standardi koji se trebaju primeniti uključuju:
1.1. Qasje në shërbime të ofruesve të internetit duke u ofruar komponente të fiksuara të sigurisë së rrjetit duhet të kontraktohen, dhe këto komponente duhet të instalohen dhe aktivizohen në pajisjet e përdorura të TIK-ut.	1.1. Internet access service providers also offering embedded network security components shall be contracted, and those components shall be installed and activated on the ICT equipment used..	1.1. Nepomične bezbednosne komponente mreže, i te komponente će biti instalirane i aktivirane na IKT opremi koja se koristi, u slušaju ugovaranja provajdera usluga za pristup na internetu.
1.2. Në rast të marrjes me qira të pajisjeve të përpunimit të të dhënave personale nga një palë e tretë profesionale, duhet të kontraktohet ofruesi i shërbimit të komponentit të sigurisë së rrjetit të kohës së fundit.	1.2. In case of renting personal data processing equipment from a professional third party, the service offering up-to-date network security components shall be contracted.	1.2. Komponentu bezbednosti mreže zadnjeg vremena koja se treba ugovoriti, u slučaju iznajmljivanja lične opreme za obradu podataka od profesionalne treće strane .
2. Në rast të përdorimit lidhjes pa tela të internetit, nuk duhet të përdoren pikat e pa enkriptuara të qasjes dhe, standardet e mëposhtme të sigurisë duhet të përputhen me:	2. In case of using wireless internet connection, non-encrypted access points shall not be used and following security standards shall be complied with:	2. U slučaju korišćenja bežične internet konekcije,ne treba da se koriste ne-enkriptirane pristupne tačke sledeći sigurnosni standardi će se poštovati:
2.1. Pikat e qasjes publike duhet të shmangen;	2.1. Public access points shall be avoided;	2.1. Javni pristupne tačke treba da se izbegavaju.

2.2. Enkriptimet e dobëta, të tilla si WEP, nuk duhet të përdoren; 2.3. Enkriptimet e forta të tilla si WPA2 ose më të mira duhet të përdoren si minimum për enkriptim. **Neni 11** **Standardet minimale të personelit në lidhje me sigurinë** 1. Përdoruesit duhet të informohen për rreziqet e mëdha të sigurisë që ekspozohen dhe trajnohen mbi përdorimin e masave të përcaktuara të sigurisë. 2. Në rast të rekrutimeve të reja, duhet të organizohet trajnimi përkatës për rreziqet e identifikuara të përpunimit të të dhënave ku këta persona do të angazhohen. 3. Personeli përkatës duhet të udhëzohet të mbajë fshehtësinë e të dhënave personale, madje edhe pas përfundimit të kontratës, dhe përfshinë: 3.1. Të gjitha të dhënat personale të qasshme gjatë ekzekutimit të kontratës;	2.2. Weak encryptions such as WEP shall not be used; 2.3. Stronger encryption such as WPA2 or better shall be used as an encryption's minimum. **Article 11** **Minimum personnel related security standards** 1. The users shall be informed of the major security risks they are exposed to, and trained to use the ordered security measures. 2. In case of new recruitments, training shall be organized correspondingly to the risks identified for data processing in which the particular persons will be engaged into. 3. The respective personnel shall be instructed to keep confidentiality of personal data, even after termination of the contract, and it covers: 3.1. All the personal data related information being accessed during execution of the contract;	2.2. Slabo enkriptiranje poput WEP se neće koristi. 2.3. Jače enkriptiranje poput WPA2 ili bolje će se koristiti kao minimum za ekriptiranje. **Neni 11** **Minimalni standardi za bezbednost osoblja** 1. Korisnici će biti obavešteni o najvećim bezbednosnim rizicima kojima su izloženi, i obučavaju se da koriste naložene mere bezbednosti. 2. U slučaju novog zapošljavanja, obuke će biti organizovane na odgovarajući način za identifikovane rizike za obradu podataka u kojima će posebne osobe biti angažovane. 3. Odgovarajuće osoblje će dobiti instrukcije da održava poverljivost ličnih podataka, čak i nakon raskida ugovora, i pokriva: 3.1. Sve informacije koje se odnose na lične podatke kojima se pristupa prilikom izvršenja ugovora;

3.2. Të gjitha mjetet dhe masat e sigurisë, veçanërisht ato të përdorura për autentikim, identifikim dhe autorizim të përdoruesit, të nevojshme për qasje në pajisjet e TIK-ut që u vihen atyre në dispozicion për përpunimin e të dhënave personale.	3.2. All security means and measures, especially those used for authentication, identification and authorisations for users necessary for accessing the ICT equipment made available to them for processing of personal data.	3.2. Sva sigurnosna sredstva i mere, naročito ona koja se koriste za potvrdu identiteta, identifikaciju i ovlašćenja za korisnike, neophodne za pristup IKT opremi koja im je dostupna za obradu ličnih podataka.
4. Të gjitha të drejtat e qasjes, në të gjitha pjesët e sistemit të TIK-ut, duhet të revokohen menjëherë pasi që përdoruesi të mos të ketë më nevojë t'i përdorë ato për përpunimin e të dhënave personale dhe pas përfundimit të kontratës, ato duhet të ndërpriten plotësisht.	4. All access rights to all parts of ICT system shall be immediately revoked after the user is no longer required to process personal data using them, and shall be terminated completely after termination of the contract.	4. Sva prava na pristup svim delovima IKT sistema biće odmah oduzeta nakon što korisniku više nije potrebno da je koristi za obradu ličnih podataka, a prestaje u potpunosti nakon raskida ugovora.
5. Trajnimi i personelit mbi sigurinë duhet të dokumentohet dhe subjekti duhet të jetë në gjendje t'ia vërtetojë Agjencisë që trajnimi është mbajtur. Organit i lejohet të zgjedhë formën e dokumentimit dhe rekomandohet që të bëhet një amendament i akteve të detyrueshme personale.	5. Personnel's training on security shall be documented and the entity shall be able to prove to the Agency that is has actually occurred. The entity is allowed to choose the form of documentation and it is advised to make it an amendment of the mandatory personal acts.	5. Obuka osoblja za sigurnost mora biti dokumentovana i subjekat mora biti u stanju da dokaže Agenciji da je održana obuka. Organu je dozvoljeno da izabere oblik dokumentacije i preporučuje se da se vrši jedan amandman obavezujućih ličnih akata.
Neni 12 **Siguria gjatë përpunimin manual**	**Article 12** **Security during manual processing**	**Član 12** **Bezbednost tokom ručne obrade**
1. Të gjitha dokumentet e përpunuara në mënyrë manuale që përmbajnë të dhëna personale duhet të mbahen të sigurta në	1. All manually processed documents containing personal data shall be kept secure in order to prevent an unlawful disclosure,	1. Sva ručno obrađena dokumenta koja sadrže lične podatke čuvaju se sigurnim u cilju sprečavanja nezakonitog otkrivanja,

mënyrë që të parandalohet shpalosja e paligjshme, shkatërrimi dhe humbja e tyre, në vendin e punës dhe/apo gjatë transferimit të tyre.	destruction and loss, both at the work place and/or while transferring thereof.	uništavanja i gubitka, kako na radnom mestu, tako i/ili tokom prenosa istih.
2. Të gjitha kopjet e kërkuara mund të vihen në dispozicion vetëm me kusht që përdorimi i tyre i mëtejshëm të jetë i gjurmueshëm, nga krijimi deri në shkatërrimin e tyre.	2. All the copies required can be made available only under the condition that their further use is traceable, from creation till destruction.	2. Sve kopije potrebne mogu biti dostupne samo pod uslovom da se njihova dalja upotreba može pratiti, od stvaranja do uništenja.
2.1. Në rast të përpunimit të përzier automatik dhe manual, dokumentet e printuara për shfrytëzim të përkohshëm duhet të kufizohen në një domosdoshmëri absolute.	2.1 In case of mixed automatic and manual processing, the temporary printouts in use shall be limited to an absolute necessity.	2.1. U slučaju mešovite automatske i ručne obrade, štampani dokumenti za privremenu upotrebu biće ograničeni na apsolutnu neophodnost.
2.2. Organi publik dhe privat duhet të jetë në gjendje të përcjellë origjinën e printimit.	2.2 The data processing public and private body shall be able to trace all printouts' originators.	2.2. Javni i privatni organ za obradu podataka moći će da uđe u trag svim izvorima ispisa.
3. Pas skadimit të periudhës ligjore kur lejohet përpunimi i të dhënave, dokumentet duhet të:	3. Upon expiry of the legal period when the data is allowed to be processed, the documents shall be:	3. Po isteku zakonskog perioda dozvoljenog za obraditi podataka, dokumenta moraju biti:
3.1. Arkivohen në rast se një detyrim i tillë ligjor ekziston; ose	3.1 Archived in case such a legal obligation exists; or	3.1. Arhivirana u slučaju da takva zakonska obaveza postoji;ili
3.2. Shkatërrohen fizikisht, në një mënyrë që e bënë të pamundur leximin e tyre; ose	3.2 Destroyed physically, in a way making them impossible to be read again;or	3.2. Fizički uništena, na način koji onemogućava da se oni ponovo čitaju; ili

3.3. Anonimizohen duke i bërë të dhënat personale me përmbajtje të palexueshme.	3.3 Anonimysed by making personal data they contain illegible.	3.3. Anoniminiziraju se čineći lične podatke koje one sadrže nečitljivim.
4. Duhet të ketë mjete të mjaftueshme dhe të arritshme teknike për shkatërrimin e dokumenteve në kopje fizike, ose me grirëse letre të poseduara nga organi publik dhe privat, ose nga shërbimi i jashtëm i kontraktuar për shkatërrim të mjeteve.	4. There should be enough and properly accessible technical means for spare paper documents destruction deployed, either by paper shredders owned by public and private body, or by contracted external media destruction service.	4. Treba da postoje dovoljno i pristupačna tehnička sredstva za uništavanje papirnih dokumenata, bilo sopstvenim sekačem papira javnog i privatnog organa ili eksternom ugovorenom uslugom.
4.1. Personeli duhet të trajnohet ti përdor ato në mënyrë që me sukses të shkatërroj materialin në letër;	4.1 Personnel shall be trained how to use them to successfully destroy paper materials;	4.1. Osoblje će biti obučeno kako da ih koristi da uspešno uništi papirne materijale.
4.2. Shportat e mbeturinave duhet të kontrollohen rregullisht nëse ato përmbajnë dokumente të pa shkatërruara;	4.2 Dustbins shall be regularly checked whether they do not contain non-shredded paper documents;	4.2. Kante za otpatke se redovno proveravaju da li sadrže neisečena papirna dokumenta;
4.3. Në rast të rreziqeve shtesë, duhet të ketë kontrolle shtesë për të siguruar se dokumentet në të vërtetë janë shkatërruar fizikisht në mënyrë të pa kthyeshme, në rast se shkatërrimi i tillë urdhërohet.	4.3 In case of additional risks, there should be additional controls in order to secure that these documents were actually physically destroyed in an irrevocable way, in case such destruction was ordered.	4.3. U slučaju dodatnih rizika, trebalo bi da postoje dodatne kontrole kako bi se osiguralo da su ovi dokumenti zaista fizički uništeni na nepovratan način, u slučaju da je naloženo takvo uništenje.
5. Kontrolle dhe masa shtesë të sigurisë duhet të zbatohen për siguri ndaj qasjes së paautorizuar, nëse dokumentet e tilla përmbajnë të dhëna të ndjeshme. Veçanërisht, këshillohet që:	5. Additional security measures and controls shall be implemented in order to secure against an unauthorised access, if these documents contain sensitive data. In particular, it is advised to:	5. Dodatne mere bezbednosti i kontrole se sprovode kako bi se sprečio neovlašćeni pristup, ako taki dokumenti sadrže osetljive podatke,. Posebno se savetuje da:
5.1. Dokumentet të ndahen fizikisht vetëm	5.1 Physically separate such documents	5.1. Fizički odvojiti takva dokumenta od

nga ato që përmbajnë të dhëna të ndieshme; 5.2. Të përdoren mjete të tjera të kontrollit të qasjes fizike, të tilla si dollapë, dosje ose dhoma të ndara; 5.3. Të zbatohet "Politika e mbajtjes së tavolinave të pastërta" nëse paragrafët 5.1 ose 2.2 të këtij neni nuk mund të zbatohen. 6. Masa organizative duhet të implementohen për të verifikuar se masat e tilla mbrojtëse për trajtimin e dokumenteve në kopje fizike zbatohen në të vërtetë, nga krijimi deri në shkatërrimin e tyre, veçanërisht për të zbuluar shkelësit e masave të sigurisë. **KAPITULLI III.** **KËRKESAT E VEÇANTA PËR ORGANET PUBLIKE DHE PRIVATE QË PËRPUNOJNË TË DHËNA ME RREZIKSHMËRI TË LARTË**	from those containing non-sensitive data only; 5.2 Use additional means of physical access control, such as separate container, files or rooms; 5.3 Execute clean-desk policy in case paragraphs 5.1 or 5.2 of this article cannot be applied. 6. Organisational means shall be implemented to verify that such safeguards for handling paper documents are actually implemented, from their creation till destruction, especially in order to be able to trace those violating the introduced security measures. **CHAPTER III.** **SPECIAL REQUIREMENST FOR PUBLIC AND PRIVATE HIGH-RISK DATA PROCESSING BODIES**	onih koji sadrze poverljive podatke; 5.2. Koristite dodatne instrumente kontrole fizičkog pristupa, kao što su odvojeni kontejner, datoteke ili sobe. 5.3. Sprovedite *"politiku čistog stola"* u slučaju da 5.1 ili 5.2 ovog člana nisu mogući. 6. Treba da se provode organizacione mere da bi se proverilo da se takve bezbednosne mere za rukovanje papirnim dokumentima zapravo sprovode, od njihovog nastanka do uništenja, posebno radi otkrivanja kršioca uvedenih mera bezbednosti. **POGLAVLJE III.** **POSEBNI USLOVI ZA JAVNE I PRIVATNE ORGANE ZA OBRADU PODATAKA VISOKOG RIZIKA**

Neni 13 Sistemi i Menaxhimit të Sigurisë së Informacionit për mbrojtjen e të dhënave personale	Article 13 Information Security Management System for personal data protection	Član 13 Sistem upravljanja bezbednošću informacija (SUBI) za zaštitu ličnih podataka
1. Ngritja dhe mirëmbajtja e SMSI-së për mbrojtjen e të dhënave personale është e detyrueshme për të gjitha organet publike dhe private që përpunojnë të dhëna me rrezikshmëri të lartë. SMSI bazohet në identifikimin e kërcënimeve dhe dobësive, analizën, vlerësimin dhe zbutjen e rreziqeve rezultuese për sigurinë e të dhënave personale, duke marrë parasysh kërcënimet dhe dobësitë e:	1. Setting-up and maintaining ISMS for personal data protection is obligatory for all public and private High-risk Processing bodies. ISMS shall be based on identification of threats and vulnerabilities, and analysis, assessment and mitigation of resulting risks to personal data security, taking into account the threats and vulnerabilities of:	1. Uspostavljanje i održavanje SUBI-ja za zaštitu ličnih podataka je obavezno za sve javne i privatne organe za obradu podataka visokog rizika. SUBI se zasniva na identifikaciji pretnji i ranjivosti, i analizi, proceni i ublažavanju rizika koji proizilaze po ličnu bezbednost podataka, uzimajući u obzir pretnje i ranjivosti:
1.1. Sistemeve të TIK-ut të përdorura për përpunimin e të dhënave personale;	1.1. ICT systems used for personal data processing;	1.1. IKT sistema korišćenih za obradu ličnih podataka;
1.2. Të gjitha formave manuale të përpunimit të të dhënave personale;	1.2. All manual forms of personal data processing;	1.2. Svih ručnih oblika obrade ličnih podataka;
1.3. Sigurisë fizike dhe mjedisore, brenda dhe jashtë objektit;	1.3. Physical and environmental security, inside and outside of the premises;	1.3. Fizičke i sigurnosti životne sredine, unutar i van prostorija,
1.4. E personelit, siç janë: gabimet njerëzore, shtrëngimet, dhe aktiviteteve kriminale.	1.4. Personnel, such as human error, coercing, and criminal activities.	1.4. Osoblja, kao što su: ljudske greške, prinude, i kriminalne aktivnosti.
2. Në rastet kur kontrolluesi përdor një procesor, ndarja e përgjegjësive ndërmjet	2. In case the controller uses a processor, division of responsibilities between the	2. Podela odgovornosti između stranaka za zaštitu ličnih podataka je eksplicitno

palëve për mbrojtjen e të dhënave personale duhet të ceket në mënyrë eksplicite në dokumentacionin që i rregullon marrëdhëniet e tyre kontraktuale. Të gjitha këto kërkesa do të plotësohen pa i paragjykuar marrëdhëniet e jashtme kontraktuale.	parties for protecting personal data shall to be explicitly stated in the documentation regulating their contractual relations. All these requirements shall be fulfilled without prejudice to outsourcing contractual relationship.	navedena u dokumentaciji koja uređuje njihove ugovorne odnose. Svi ovi zahtevi biće ispunjeni bez prejudiciranja ugovornog odnosa - outsourcing.
3. Kur kontrolluesi përdor përpunues me rrezik të ulët, vetëm pjesët përkatëse të SMSI-it të cilat zbatohen, duhet ti komunikohen atij dhe duhet të jenë ligjërisht të detyrueshme në kontratën për kontraktimin e përpunimit të të dhënave.	3. When the controller uses a low-risk processor, only the corresponding parts of the ISMS which are actually applicable shall be communicated to it, and legally binding in the data processing outsourcing contract.	3. Kada kontrolor koristi obrađivača niskog rizika, biće saopšteni jedino odgovarajući delovi SUBI-ja koji su zapravo primenljivi, i pravno obavezujući u outsourcing ugovoru za obradu podataka.
4. Gjatë strukturimit të SMSI-së, vëmendje e veçantë duhet t'i kushtohet standardeve të sigurisë teknike të informacionit, kodeve të praktikës së mirë, rekomandimeve dhe udhëzimeve specifike të miratuara nga Agjencia.	4. During ISMS structuring, special attention should be paid to the technical standards of information security, codes of good practice, specific recommendations and instructions adopted by the Agency.	4. Tokom struktuiranja SUBI, posebna pažnja treba da se obrati standardima tehničke bezbednosti informacije, kodeksu dobre prakse, spcifičnim preporukama i uputstvima usvojenih od strane Agencije.
5. Mbikëqyrja e SMSI-it dhe mirëmbajtja e dokumentacionit është detyrë e Zyrtarit të Mbrojtjes së të Dhënave, ose e një personi tjetër të emëruar për mbikqyrje të sigurisë në rast se një zyrtar i tillë nuk është i emëruar. Ky dokumentacion i SMSI-së duhet të jetë në dispozicion të Agjencisë me kërkesë të saj pa vonesë, në lidhje me pjesën e saj që ka të bëjë me mbrojtjen e të dhënave	5. Supervision of ISMS and its documentation's maintenance is the duty of the Data Protection Official, or of another person appointed for security supervision, in case that such an official is not appointed. This ISMS's documentation must be available to the Agency at its request without delay, in its part related to personal data protection.	5. Nadzor SMSI i održavanje njegove dokumentacije je dužnost zvaničnika za zaštitu podataka , ili drugog lica imenovanog za bezbednost u slučaju da se takav zvaničnik ne imenuje. Ova dokumentacija mora biti dostupna Agenciji na njen zahtev, bez odlaganja, u vezi sa delom od koje ima veze sa zaštitom ličnih podataka.

personale.		
Neni 14 **Përmbajtja e SMSI-së**	**Article 14** **The content of ISMS**	**Član 14** **Sadržaj SUBI**
1. SMSI veçanërisht duhet të përfshijë:	1. The ISMS shall include in particular:	1. SUBI naročito treba obuhvati:
1.1. PSI-në, që mbulon sigurinë e përpunimit të të dhënave personale;	1.1. ISP, covering personal data processing security,	1.1. PBI, koje pokriva bezbednost obrade ličnih podataka,
1.2. Rregullat e auditimit dhe inspektimit për sigurinë e sistemit të dosjeve të të dhënave personale;	1.2. The audit and inspections rules for the personal data filing system's security;	1.2. Pravila revizije i inspekcije za bezbednost sistema za arhiviranje ličnih podataka;
1.3. Organizimin e sigurisë së informacionit, duke përcaktuar masa mbrojtëse të hollësishme për mbrojtjen e informacionit dhe sistemet e tyre të përpunimit ndaj kërcënimeve të identifikuara.	1.3. Organization of information security, specifying detailed safeguards deployed for protecting information and its processing systems against identified threats.	1.3. Organizaciju informacione bezbednosti, navodeći detaljne mere zaštite raspoređene za zaštitu informacija i njegove sisteme obrade za borbu protiv identifikovanih pretnji.
1.4. Udhëzime të hollësishme të sigurisë që mbulojnë fushat specifike, të cilat shërbejnë si dokumente ekzekutive në PSI dhe mbulojnë:	1.4. Detailed security instructions covering specific areas, working as executive documents to the ISP, covering:	1.4. Detaljna uputstva bezbednosti obuhvataju posebne oblasti, koje funkcionišu kao izvršna dokumenta PBI-ju, pokrivajući:
1.4.1. Rolet dhe përgjegjësitë personale dhe/ose kontraktuale duhet të përcaktohen për të gjitha masat e veçanta të sigurisë;	1.4.1. Roles and personal and/or contractual responsibilities shall be appointed to all particular security measures;	1.4.1. Uloge i lične i/ili ugovorne obaveze će biti određene svim konkretnim merama bezbednosti;

1.4.2. Një grup përkatës i kontrolleve duhet të zbatohet për secilën masë;	1.4.2. An appropriate set of controls shall be applied to each measure;	1.4.2. Odgovarajući skup kontrola će se primenjivati za svaku meru.
1.4.3. Rregullat e bashkëpunimit dhe ndërveprimit udhëzohen kudo që ato janë të zbatueshme.	1.4.3. Co-operation and interaction rules shall be also instructed wherever applicable.	1.4.3. Plavila saradnje i interakcije biće takođe upućena gde je potrebno.
1.5. Menaxhimin e aseteve, duke përditësuar inventarin e të gjitha veglave të përpunimit dhe klasifikimi i kritereve të sigurisë që përcakton se çfarë, pse dhe si duhet të mbrohen;	1.5. Assets management, by updating the inventory of all processing tools and the classification of security criteria defining what, why and how is to be safeguarded;	1.5. Upravljanje imovinom, ažuriranjem inventara svih sredstava obrade i klasifikacije bezbednosnih kriterijuma koji definišu šta, zašto i kako treba da se zaštiti;
1.6. Sigurinë e burimeve njerëzore, duke marrë masat e sigurisë për punonjësit e organeve publike dhe private;	1.6. Human resources security, by taking security measures for employees of public and private bodies;	1.6. Bezbednost ljudskih resursa preduzimanjem mera bezbednosti za zaposlene, koji dolaze i odlaze iz javnih i privatnih organa za obradu podataka;
1.7. Sigurinë fizike dhe mjedisore, duke mbrojtur objektet kompjuterike;	1.7. Physical and environmental security, by protecting the computer facilities;	1.7. Fizičku i bezbednost životne sredine, putem zaštite kompjuterskih objekata;
1.8. Menaxhimin e komunikimeve dhe operacioneve duke kontrolluar sigurinë teknike në sistemet dhe rrjetet kompjuterike;	1.8. Management of communications and operations by controlling the technical security in computer systems and networks;	1.8. Upravljanje komunikacijama i operacijama kontrolisanjem tehničke bezbednosti na kompjuterskim sistemima i mrežama;
1.9. Kontrollin e qasjes, duke kufizuar të drejtat e qasjes në rrjete, sisteme, aplikacione, funksione dhe të dhëna;	1.9. Access control, by restricting access rights to networks, systems, applications, functions and data;	1.9. Kontrolu pristupa ograničavanjem prava pristupa mrežama, sistemima, aplikacijama, funkcijama i podacima;

1.10. Përvetësimin, zhvillimin dhe mirëmbajtjen e sistemeve të përpunimit të informacionit duke ngritur sigurinë në aplikacione;	1.10. Acquisition, development and maintenance of information processing systems by building security into applications;	1.10. Nabavku, razvoj i održavanje sistema obrade informacija putem izgradnje bezbednosti u aplikacijama;
1.11. Menaxhimin e shkeljeve të sigurisë së informacionit (të referuara si incidente) duke parashikuar dhe reaguar në mënyrë adekuate ndaj ngjarjeve të tilla;	1.11. Management of information security breaches (referred to as incidents) by predicting and counteracting appropriately against such events;	1.11. Upravljanje narušavanjima bezbednosti informacija (referisanim kao incidenti) putem predviđanja incidenata i adekvatnog suprotstavljanja takvim događajima;
1.12. Vazhdimësia e menaxhimit të veprimtarisë duke mbrojtur, mirëmbajtur dhe rikthyer proceset dhe sistemet kritike;	1.12. Business continuity management by protecting, maintaining and recovering critical processes and systems;	1.12. Upravljanje poslovnim kontinuitetom putem zaštite, održavanja i oporavka kritičnih procesa i sistema;
1.13. Sigurimi i pajtueshmërisë me politikat specifike të sigurisë së informacionit, standardet, ligjet dhe rregulloret, sidomos ato specifike për sektorë.	1.13. Ensuring compliance with specific information security policies, standards, laws and regulations, especially those sector specific ones.	1.13. Obezbeđivanje usaglašavanja sa specifičnim politikama bezbednosti informacija, standardima, zakonima i propisima, posebno onih specifičnih za sektor.
2. SMSI-i duhet të përmbajë rregullore të detajuara të sigurisë së brendshme (dokumente ekzekutive për PSI-i), të cilat specifikojnë se si zbatohen dhe kontrollohen parimet e përgjithshme të sigurisë së PSI-së në kushtet e veçanta të përpunimit të sistemit të dosjeve. Ato në veçanti duhet të përfshijnë:	2. The ISMS shall contain detailed internal security regulations (executive documents to the ISP) which shall specify how the general security principles of the ISP are implemented and checked under the particular processing conditions of the operated filing system. It shall include in particular:	2. SUBI sadrži detaljne odredbe unutrašnje bezbednosti (izvršni dokumenti za PBI) koje određuju način na koji su opšti principi bezbednosti PBI-ja sprovedeni i provereni pri određenim uslovima obrade operativnih sistema arhiviranja. Oni posebno sadrže:
2.1. Analizën dhe vlerësimin e rreziqeve për nivelin e caktuar të komponentit të	2.1. Risks analysis and assessment on the level of particular component of the data	2.1. Analizu i Procenu rizika na nivou posebne komponente sistema za obradu

sistemit të përpunimit të të dhënave; 2.2. Përshkrimin e masave teknike, organizative dhe të lidhura me personelin të përcaktuara në SMSI-së dhe përdorimin e tyre nën kushte të veçanta; 2.3. Shkallën e kompetencave dhe përshkrimin e veprimtarive të lejuara për individët që kanë të drejtë të qasjes, mënyrën e identifikimit dhe validimit të tyre për qasje në sistemin e dosjeve, 2.4. Detyrimet e personave përgjegjës dhe të Zyrtarit të Mbrojtjes së të Dhënave (apo personit të emëruar për sigurinë e të dhënave personale në zyrtari nuk është emëruar); 2.5. Mënyrën, formën dhe periudhën e aktiviteteve të auditimit dhe inspektimit të brendshëm të fokusuar në vlerësimin e sistemit të dosjeve dhe sigurinë e sistemit të përpunimit. 2.6. Procedurat e rimëkëmbjes në rast fatkeqësie për riparimin e situatave të jashtëzakonshme të tilla si prishjet, dështimet kritike të personelit dhe teknologjisë, duke përfshirë mjetet për	processing system; 2.2. Description of the technical, organizational, and personnel related measures defined in the ISMS and their use for this particular conditions; 2.3. The extent of powers and description of the activities permitted to individual persons entitled to access rights, the manner of their identification and authentication in accessing the filing system, 2.4. Liabilities of persons in charge and of the Data Protection Official (or of another appointed person in charge of personal security in case such an Official was not appointed); 2.5. The manner, form and periodicity of internal audit and inspection activities focused on assessment of the filing system's and it processing system's security. 2.6. Disaster recovery procedures for servicing extraordinary situations such as breakdowns, critical failures of personnel and technology, including mitigation means and preventive measures to limit	podataka, 2.2. Opis tehničkih, organizacionih, kadrovskih mera definisanih u SUBI-ju i njihovo korišćenje za ove posebne uslove, 2.3. Obim ovlašćenja i opis aktivnosti dozvoljenih pojedinim osobama koje imaju pravo na pristup, način njihove identifikacije i provere identiteta pri pristupu sistemu arhiviranja, 2.4. Obaveze lica zaduženih i službenika za zaštitu podataka (ili drugog imenovanog lica zaduženog za ličnu bezbednost u slučaju da takav službenik nije imenovan). 2.5. Način, oblik i periodičnost interne revizije i inspekcijskih aktivnosti fokusiranih na procenu sistema arhiviranja i njegovu bezbednost sistema obrade. 2.6. Procedure za oporavak od katastrofa za servisiranje vanrednih situacija, kao što su havarije, kritični propusti osoblja i tehnologije, uključujući sredstva za ublažavanje i preventivne mere za

zbutje dhe masat parandaluese për të kufizuar ndikimin e tyre dhe parandalimin e ngjarjeve të tilla në të ardhmen.	their impact and prevent such events in future.	ograničavanje njihovog uticaja i sprečavanje ovakvih događaja u budućnosti.
2.6.1. Infrastruktura e rimëkëmbjes në rast fatkeqësie duhet të vihet në dispozicion;	2.6.1. Disaster recovery infrastructure shall be also made available;	2.6.1. Biće dostupna infrastruktura za oporavak od katastrofa;
2.6.2. Proceset kritike duhet të identifikohen dhe të trajtohen në mënyrë adekuate;	2.6.2. Critical processes shall be properly identified and handled;	2.6.2. Kritični procesi će biti odgovarajuće identifikovani i upravljani;
2.6.3. Testimi periodik i masave të hartuara është i detyrueshëm;	2.6.3. Periodic testing of the drafted measures is mandatory;	2.6.3. Periodično testiranje izrađenih mera je obavezno;
2.6.4. Në rast të dështimit për tu testuar, sistemi i tillë duhet të konsiderohet si jo i zbatueshëm.	2.6.4. In case of failure to test, such a system is to be considered as non-implemented.	2.6.4. U slučaju da ne uspete u testiranju, takav sistem treba smatrati nesprovedenim.
2.6.5. Në rast se rezultati i vlerësimit të rrezikut kërkon një aranzhim më kompleks, atëherë duhet të aplikohet një rimëkëmbje e thjeshtë në rast fatkeqësie, e cila mbulon vetëm perspektivën e sigurisë së TIK-ut, pastaj vendoset sistemi i plotë i vazhdimësisë së menaxhimit të veprimtarisë, që mbulon:	2.6.5. In case the risk assessment's outcome asks for a more complex arrangement, then a simple disaster recovery which covers the ICT security perspective only, then a fully blown business continuity management system shall be established, covering:	2.6.5. U slučaju da ishod procene rizika traži složenija uređenja, onda treba uspostaviti jednostavan oporavak sistema nakon katastrofa, koji samo pokriva IKT bezbednosnu perspektivu, i uspostaviti potpuno razvijen Sistem upravljanja kontinuitetom poslovanja, pokrivajući:
2.6.5.1. Rimëkëmbjen e TIK-ut në rast fatkeqësie;	2.6.5.1. Disaster recovery for ICT;	2.6.5.1. Oporavak sistema nakon katastrofa za IKT;

2.6.5.2. Menaxhimin e personelit, komunikimin me subjektet e të dhënave dhe mediat, si dhe mjetet tjera të nevojshme për të parandaluar prishjet e pakthyeshme të subjektit, dhe kthimin e suksesshëm të saj në funksionim normal.	2.6.5.2. Management of personnel, communication with data subjects and media, and other means required to prevent an irrevocable breakdown of the entity, and its successful return to normal operations.	2.6.5.2. Upravljanje osobljem, komunikacija sa nosiocima podataka i medijima i drugim sredstvima potrebnim za sprečavanje neopozivog kvara ovog subjekta, i njegov uspešan povratak u normalan rad.
3. SMSI-si duhet të funksionojnë në përputhje me aktet ligjore, standardet teknike për sistemet e sigurisë së TIK-ut, rregullat e praktikës së mirë në fushën e sigurisë së informacionit, si dhe rekomandimet e lëshuara nga:	3. ISMS shall function in compliance with the legal acts, technical standards for ICT security systems, rules of good practice in the information security field, and the recommendations issued by:	3. SUBI će funkcionisati u skladu sa zakonskim i podzakonskim aktima na snazi, tehničkim standardima za IKT sigurnosne sisteme, pravilima dobre prakse u oblasti bezbednosti informacija, i preporukama koje izdaju:
3.1. Agjencia;	3.1. The Agency;	3.1. Agencija;
3.2. Organizatat e themeluara private dhe publike profesionale industriale, të tilla si përfaqësitë e sektorëve bankar, telekomunikacionit, sigurimit, sigurimit social dhe sektorët e kujdesit shëndetësor.	3.2. Established private and public professional industrial organizations, such as in particular representations of banking, telecommunications, insurance, social security and health care sectors.	3.2. Osnovane privatne i profesionalne javne industrijske organizacije, kao što su u pojedinim institucijama bankarstva, telekomunikacija, osiguranja, socijalne sigurnosti i sektora zdravstvene zaštite.
4. SMSI duhet të jetë i përshtatshëm për nivelin e identifikuar të kërcënimeve, dobësive dhe rreziqeve të cilave u ekspozohen sistemet e përpunimit të të dhënave personale:	4. The ISMS should be adequate to the identified level of threats, vulnerabilities and risks which personal data processing systems are exposed to:	4. SUBI treba da bude adekvatan za identifikovani nivo pretnji, ranjivosti i rizika kojima su izloženi sistemi obrade ličnih podataka:

4.1. Në rast se një auditim zbulon mangësi, mënyra për ti zbutur ato duhet të caktohet nga Zyrtari për Mbrojtjen e të Dhënave, ose nga personi tjetër i emëruar për sigurinë në ras se Zyrtari nuk është i emëruar, së bashku me menaxhimin e lartë dhe zbatohet pa vonesë të konsiderueshme.	4.1. In case an audit discovers some deficiencies, the way to mitigate them shall be agreed by the Data Protection Official or by the other appointed person in charge of personal security in case such an Official was not appointed, with the top management, and implemented without substantial delay.	4.1. U slučaju da revizija otkrije neke nedostatke, način da se oni ublaže biće dogovoreni od strane službenika za zaštitu podataka, ili od strane drugog imenovanog lica zaduženog za ličnu bezbednost u slučaju da takav službenik nije bio postavljen, sa najvišim rukovodstvom, i biće sproveden bez značajnog odlaganja.
Neni 15 **Analiza dhe vlerësimi gjatë plotësimit të sistemit të dosjeve**	**Article 15** **Analysis and assessment of filing system security**	**Neni 15** **Analiza dhe vlerësimi i sigurisë së sistemit të dosjeve**
1. Analiza dhe vlerësimi i sigurisë së sistemit të dosjeve të të dhënave personale nënkupton një vlerësim të detajuar të gjendjes së sigurisë që përbëhet nga:	1. Personal data filing system security analysis and assessment means a detailed evaluation of the state of security comprising in particular:	1. Analiza i procena bezbednosti sistema za arhiviranje ličnih podataka označava detaljnu ocenu stanja bezbednosti koje sadrži posebno:
1.1. Analiza e rrezikut, ku identifikohen kërcënimet të cilat ndikojnë në pjesë të veçanta të sistemit të dosjeve, që mund të shkelin sigurinë ose funksionalitetin e tij. Rezultati i analizës dhe vlerësimit të rrezikut duhet të jenë lista e:	1.1. Risk analysis, in which the threats affecting individual parts of the filing system, capable of violating its security or functionality are identified. The outcome of the risk analysis and assessment shall be a list of:	1.1. Analiza rizika, u kojoj se identifikuju pretnje koje utiču na pojedinačne delove sistema arhiviranja, sposobne za kršenje njene bezbednosti ili funkcionalnosti identifikovane. Ishod analize i procene rizika biće spisak:
1.1.1. kërcënimeve që mund të rrezikojnë konfidencialitetin, integritetin dhe disponueshmërinë e të dhënave personale të përpunuara, përderisa gjithashtu duhet të cekë	1.1.1. threats that could endanger confidentiality, integrity and availability of personal data processed, while it shall also state the extent of the possible risk;	1.1.1. pretnji koje mogu ugroziti poverljivost, integritet i dostupnost obrađenih ličnih podataka, a takođe će navesti obim mogućeg rizika;

shkallën e rrezikut të mundshëm; 1.1.2. propozimeve për masat që eliminojnë ose minimizojnë ndikimin e rrezikut dhe një listë të rreziqeve të mbetura. 1.2. Aplikimi i standardeve të sigurisë dhe përcaktimi i metodave dhe mjeteve tjera të mbrojtjes së të dhënave personale; 1.3. Vlerësimi i përputhshmërisë së masave të propozuara të sigurisë me standardet e aplikuara të sigurisë, **Neni 16** **Analiza e Ndikimit në Privatësi** 1. Analiza e rreziqeve dhe vlerësimi para dhe gjatë përpunimit të të dhënave me rrezikshmëri të lartë, gjithashtu duhet të përmbajnë: 1.1. analizën e ndikimit të të dhënave personale, siç shihet nga këndvështrimi i subjektit, të dhënat e së cilës përpunohen. 2. Para përpunimit të të dhënave personale, kontrolluesi ose përpunuesi duhet të bëjë një vlerësim të ndikimit të operacioneve të	1.1.2. Proposals of the measures to eliminate or minimize the risk impact and a list of residual risks, 1.2. Application of security standards and determination of other methods and means of protecting personal data; 1.3. The compliance evaluation of the proposed security measures with the applied security standards. **Article 16** **Privacy Impact Analysis** 1. The risks analysis and assessment prior and during any high risk data processing, shall also contain: 1.1. Personal data impact analysis, as viewed from the data subject's perspective whose data are being processed. 2. Prior to processing of personal data, the Controller or the Processor shall carry out an assessment of an impact of the envisaged	1.1.2. predloga za mere za otklanjanje ili umanjenje uticaja rizika i spisak preostalih rizika; 1.2. Primena bezbednosnih standarda i određivanje drugih metoda i sredstava za zaštitu ličnih podataka, 1.3. Evaluacija usklađenosti predloženih mera bezbednosti sa primenjenim bezbednosnim standardima. **Neni 16** **Analiza Uticaja u Privatnost** 1. Analiza i procena rizika tokom obrade ličnih podataka visokog rizika, takođe treba da sadrže: 1.1. Analizu uticaja na lične podatke, posmatrano sa stanovišta nosioca podataka čiji se podaci obrađuju. 2. Pre obrade ličnih podataka, kontrolor ili obrađivač vrši procenu uticaja predviđenih postupaka obrade na zaštitu ličnih

parapara të përpunimit për mbrojtjen e të dhënave personale, duke identifikuar se ku operacionet e tilla të përpunimit mund të paraqesin rreziqe specifike për të drejtat dhe liritë e subjektit të të dhënave duke u mbështetur në natyrën, cilësitë, ose qëllimet e tyre.	processing operations on the protection of personal data thus identifying where such processing operations which are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes.	podataka, identifikujući gde će takvi postupci obrade verovatno predstavljati konkretne opasnosti za prava i slobode nosioca podataka zbog njihove prirode, kvaliteta ili svrhe.
Neni 17 **Politika për Sigurinë e Informacionit**	**Article 17** **Information Security Policy**	**Član 17.** **Politika bezbednosti informacija**
1. PSI-ja specifikon objektivat themelore të sigurisë që duhet të arrihen për mbrojtjen e sistemit të dosjeve të të dhënave personale kundër shkeljes së sigurisë së tij, në mënyrë të veçantë ai duhet të:	1. The ISP specifies the basic security objectives that must be achieved for protection of the personal data filing system against violation of its security and in particular it shall:	1. PBI precizira osnovne bezbednosne ciljeve koji se moraju ostvariti za zaštitu sistema arhiviranja ličnih podataka za borbu protiv kršenja njegove bezbednosti, a posebno PBI će:
1.1. përshkruajë sistemin e dosjeve dhe lidhjen e tij me shkeljet e mundshme të sigurisë;	1.1. Describe the filing system and its relation to the possible security violations;	1.1. opisati sistem arhiviranja i njegov odnos sa mogućim kršenjima bezbednosti;
1.2. specifikojë objektivat e sigurisë themelore dhe masat minimale të kërkuara për siguri;	1.2. specify the objectives of basic security and the minimum security measures required;	1.2. navesti ciljeve osnovne bezbednosti i potrebne minimalne bezbednosne mere;
1.3. specifikojë masat teknike, organizative dhe të lidhura me personelin për mbrojtjen e të dhënave personale në sistemin e dosjeve dhe mënyrën e përdorimit të tyre;	1.3. specify the technical, organizational and personnel related measures for safeguarding personal data in the filing system and the manner of their use,	1.3. navesti tehničke, organizacione i kadrovske mere za čuvanje ličnih podataka u sistemu arhiviranja i način njihovog korišćenja;

1.4. përcaktojë kufijtë duke përcaktuar rreziqet e mbetura.	1.4. define the limits determining the residual risks.	1.4. definisati granice koje određuju preostale rizike.
2. PSI duhet të përmbajë deklaratën e angazhimit të menaxhmentit për të mirëmbajtur nivelin e duhur të sigurisë, si dhe udhëzimet mbi drejtimet kryesore dhe mjetet e caktuara teknike dhe organizative që do të përdoren për të arritur këtë qëllim.	2. The ISP shall contain declaration of the top management's commitment to maintain a proper security level, and instructions on major directions and particular technical and organisational means to be used to achieve this goal.	2. PBI treba da sadrži izjavu o posvećenosti top menadžmenta da održi odgovarajući nivo bezbednosti, i uputstva o glavnim pravcima i određenim tehničkim i organizacionim sredstvima koja će se koristiti za postizanje tog cilja.
2.1. PSI duhet të vihet në dispozicion për të gjithë personat përgjegjës për mbrojtjen e sigurisë, duke përfshirë personelin e vetë organit publik dhe privat dhe palëve të treta të kontraktuara si përpunues të të dhënave.	2.1. This ISP document shall be made available to all responsible for maintaining security, including public and private body personnel and third parties contracted as data processors.	2.1. PBI treba da bude dostupan svima odgovornima za održavanje bezbednosti, uključujući sopstveni kadar i treća lica ugovorena kao obrađivači podataka.
2.2. Përshkrimet e hollësishme të politikave të veçanta, të cilat përbëjnë sistemin e sigurisë, duhet të:	2.2. Detailed descriptions of specific policies, which comprise the security system itself, shall be:	2.2. Detaljni opisi specifičnih politika, koje čine sami bezbednosni sistem, jesu:
2.2.1. Mos jenë të përfshira në dokumentin e PSI-së;	2.2.1. Not included in this ISP document;	2.2.1. Neuključeni u ovaj dokument o PBI-ju
2.2.2. Udhëzojë mbi udhëzimet dhe procedurat e veçanta ekzekutive për SMSI, duke ndjekur serinë e standardeve ISO-27000;	2.2.2. Instructed in specific ISMS executive instructions, and procedures, following the ISO-27000 series standards	2.2.2. Opisani u specifičnim izvršnim uputstvima i procedurama SUBI-ja, sledeći seriju standarda ISO-27000
2.2.3. Të vihen në dispozicion sipas	2.2.3. Made available on the need-to-	2.2.3. Dostupni kada je potrebno

"nevojës për njohuri" të atyre që janë përgjegjës për ekzekutimin dhe mbikëqyrjen e tyre.	know basis to those responsible for their execution and supervision.	znati o njima onima koji su odgovorni za njihovo izvršenje i nadzor.
3. PSI-ja duhet të hartohet, zbatohet dhe mirëmbahet në përputhje me rregullat e sigurisë së informacionit, të përcaktuara në aktet ligjore dhe aktet e ratifikuara ndërkombëtare, i rekomanduar nga standardet e përcaktuara të sigurisë siç janë seria e ISO-27000 dhe rekomandimet e Agjencisë.	3. The ISP shall be drafted, implemented and maintained in compliance with the rules of information security, as defined in the legal acts and ratified international acts, recommended by the established security standards such as ISO-27000 series, as well as recommendations of the Agency.	3. PBI će biti izrađeni, sprovedeni i održavani u skladu sa pravilima o bezbednosti informacija, kao što je definisano u pravnim aktima i ratifikovanim međunarodnim aktima, preporučenim prema utvrđenim bezbednosnim standardima, kao što su ISO-27000 serije, kao i preporukama Agencije.
3.1. Analiza e rreziqeve dhe vlerësimi duhet të bëhet komponentë përbërës i PSI-së.	3.1. The risks analysis and assessment shall be made an integral component of the ISP.	3.1. Analiza rizika i procena biće integralna komponenta PBI-ja.
3.2. Dokumenti i PSI-së duhet të specifikojë në mënyrë të qartë objektivat e sigurisë dhe të përcaktojë masat teknike, organizative dhe të lidhura me personelin të nevojshme për identifikimin e kërcënimeve dhe zbutjen e rreziqeve që ndikojnë në sistemet e dosjeve.	3.2. The ISP document shall clearly specify the security objectives and define the technical, organizational and personnel related measures necessary for identification of threats and mitigation of risks affecting the filing systems.	3.2. PBI dokument će jasno odrediti ciljeve bezbednosti i definisaće tehničke, organizacione i kadrovske mere neophodne za identifikaciju pretnji i ublažavanje rizika koji utiču na sistem arhiviranja.
4. PSI-ja duhet të përkufizohet në termat e mëposhtëm:	4. The ISP shall be defined in terms of the following:	4. PBI će biti definisan u sledećem smislu:
4.1. *Konfidencialiteti*, duke siguruar që të dhënat janë të qasshme vetëm për personat e autorizuar;	4.1. *Confidentiality*, ensuring that data is accessible to authorized persons only;	4.1. *Poverljivost*, osiguravajući da su podaci dostupni samo ovlašćenim licima,

4.2. *Integriteti*, duke siguruar se të dhënat janë të sakta dhe të plota dhe ruajtjen e metodave të përpunimit;	4.2. *Integrity,* ensuring the data is accurate and complete, and preserving the processing methods;	4.2. *Integritet*, osiguravajući da su podaci tačni i potpuni, i očuvanje metoda obrade;
4.3. *Disponueshmëria*, duke siguruar qasje të përdoruesve të autorizuar në të dhënat dhe të sistemet e përpunimit;	4.3. *Availability*, ensuring access of authorized users to data and to processing systems;	4.3. *Dostupnost*, osiguravajući pristup ovlašćenim korisnicima podataka i sistemima obrade;
4.4. Përgjegjshmëria e sistemeve të TIK-ut të përdorura për përpunimin e të dhënave dhe të personelit që operon me to, duke garantuar se çdo aktivitet/ operacion i tyre në të dhëna është i gjurmueshëm dhe i audituesshëm.	4.4. Accountability of ICT systems used for data processing and of the personnel operating them, guaranteeing that their every activity/operation on the data is traceable and auditable.	4.4. Odgovornost IKT sistema korišćenog za obradu podataka i osoblja koje rukuje njima, garantujući da je njihova svaka aktivnost/operacija na podacima praćena i proverena.
5. Gjatë zbatimit të dispozitave të këtij Neni, pikat në vijim duhet të adresohen veçanërisht nga PSI-ja:	5. While implementing the provisions of this Article, the following issued shall be specially addressed by the ISP:	5. Pri sprovođenju odredaba ovog člana, sledeća pitanja biće posebno rešena PBI-jem:
5.1. Përpunimi i të dhënave të ndjeshme;	5.1. Sensitive data processing;	5.1. Obrada osetljivih podataka;
5.2. Performanca aktuale e menaxhimit të drejtave të qasjes;	5.2. Access rights management's actual performance;	5.2. Upravljanje pravima na pristup stvarnog učinka;
5.3. Rreziqet që vijnë nga qasja në rrjetet publike, veçanërisht nga interneti;	5.3. Risks coming from the access to public networks, especially from the Internet;	5.3. Rizici koji dolazi iz pristupa javnim mrežama, posebno sa interneta;
5.4. Menaxhimi i përpunimit portativ;	5.4. Portable processing's management;	5.4. Upravljanje prenosivom obradom;

5.5. Menaxhimi i të gjitha llojeve të qasjes nga largësia.	5.5. All sorts of remote access's management.	5.5. Upravljanje svim vrstama udaljenog pristupa
Neni 18 **Auditimi i SMSI-së dhe bashkëpunimi me Agjencinë**	**Article 18** **Auditing ISMS and cooperation with the Agency**	**Član 18** **Revizija SUBI-ja i saradnja sa Agencijom**
1. Auditimi i SMSI duhet të kryhet:	1. ISMS audit is to be performed:	1. Revizija SUBI-ja treba da bude izvršena:
1.1. në organin publik, i cili nuk është i certifikuar me ISO-27001, në përputhje me ligjin për Auditim të Brendshëm;	1.1. At the public body not certified on ISO-27001, in accordance with the Internal Audit Law;	1.1. kod javnog organa koji nije certifikovan sa ISO-27001, u skladu sa Zakonom o unutrašnjoj reviziji;
1.2. në organin privat, i cili nuk është i certifikuar me ISO-27001, në përputhje me procedurat e brenshme të auditimit dhe të përshtatshmërisë;	1.2. At the private body not certified on ISO-27001, in accordance with its internal procedures concerning audit and compliance;	1.2. kod privatnog organa koji nije certifikovan sa ISO-27001, u skladu sa Zakonom o unutrašnjoj reviziji;
1.3. në organin publik ose privat të certifikuar me ISO-27001, në përputhje me orarin e mirëmbajtjes sipas certifikatës.	1.3. At a public or private body certified on ISO-27001, in accordance with its certification's maintenance schedule.	1.3. kod javnog i privatnog organa koji su certifikovani sa ISO-27001, u skladu sa rasporedom sadrzavanja prema certifikatu.
2. Të gjitha këto auditime duhet të bëhet jo më pak se një herë në vit.	2. All such audit shall be performed not less than once a year.	2. Sva ove revizije treba da se vrse ne manje od jedanom godisnjem.
3. Në përputhje me Nenin 46 dhe 48 të Ligjit për Mbrojtjen e të Dhënave Personale, Agjencia në çdo kohë mund të kërkoj nga organi publik dhe privat që bënë përpunimin e të dhënave personale të dëshmoj shkallën	3. In accordance with the Articles 46 and 48 of Law on Protection of Personal Protection, the Agency may, at any time request the public and private personal data processing body to prove the extent and the contents of	3. U skladu sa članovima 46. i 48. Zakona o zaštiti ličnih podataka, Agencija može, u svakom trenutku, zatražiti od javnog i privatnog organa koji obrađuje lične podatke da dokaže obim i sadržaj tehničkih,

dhe përmbajtjen e masave përkatëse të sigurisë teknike, organizative dhe të masave të ndërlidhura me personelin, përmes raportit vjetor të vlerësimit nga auditimi i realizuar nga organi publik dhe privat përpunues.	the technical, organizational and personnel related security measures, through an annual assessment report from an audit performed by the public and private processing body.	organizacionih i kadrovskih mera bezbednosti, kroz godišnji izveštaj o proceni iz revizije koju je izvršio javni i privatni organ za obradu podataka.
3.1. Organet publike dhe private të përpunimit të të dhënave duhet të dorëzojnë raportin e vlerësimit brenda pesëmbëdhjetë (15) ditëve nga dita e kërkesës;	3.1. Public and private data processing bodies shall submit the assessment report within fifteen (15) days from the day of the request;	3.1. Javni i privatni organi za obradu podataka dostavlja izveštaj o proceni u roku od petnaest (15) dana od dana podnošenja zahteva;.
3.2. Nëse raporti i vlerësimit nuk dorëzohet në kohë, Agjencia do të kërkoj nga organi publik dhe privat për përpunimin e të dhënave personale që të realizoj auditim të ri me shpenzimet e saja dhe të dorëzoj raportin e vlerësimit brenda tre (3) muajve.	3.2. Should the assessment report not be provided on time, the Agency requests the public and private personal data processing body to conduct a new audit on its own expense and submit the assessment report within three (3) months.	3.2. Ukoliko izveštaj o proceni ne može biti obezbeđen na vreme, Agencija će tražiti da javni i privatni organ za obradu ličnih podataka izvrši novu reviziju o svom trošku i dostavi izveštaj o proceni u roku od tri (3) meseca.
4. Auditimi i SMSI-së mund të realizohet vetëm nga një auditor i pavarur, i brendshëm ose i jashtëm, i paanshëm dhe profesionalisht i kualifikuar, i cili nuk ka marrë pjesë në zhvillimin, zbatimin dhe funksionalizimin e SMSI-së në atë organ publik apo privat.	4. Auditing of the ISMS may only be performed by an independent, internal or extarnal, impartial and professionally qualified auditor, who did not participate in the development, implementation and running of the ISMS in that public and private body.	4. Reviziju SUBI može obavljati samo nezavisni, interni ili eksterni, nepristrasni- i profesionalno kvalifikovani revizor, koji nije učestvovao u razvoju, sprovođenju i vođenju SUBI u tom javnom ili privatnom organu .
5. Edhe nëse organi publik dhe privat nuk	5. Even if the public and private body has not decided to be certified on this security	5. Iako javni i privatni organ nije odlučio da se sertifikuje matrica kontrola koja će

ka vendosur që të certifikohet me standard të sigurisë, matrica e kontrolleve për përdorim të auditimeve dhe inspektimeve të brendshme duhet të bazohet në standardin e sigurisë teknike ISO-27001, dhe duhet të përfshijë:	standard matrix of controls to be used for internal audits and inspections shall be based on the ISO-27001 technical security standard, and it shall include:	se koristiti za unutrašnju reviziju i inspekcije će se zasnivati na standardu tehničke bezbednosti ISO-27001, čak i ako subjekat nije odlučio da bude sertifikovan po ovom standardu bezbednosti, i treba da sadrži:
5.1. Identifikimin, vlerësimin dhe trajtimin e rreziqeve të mëdha për shkak të të gjitha formave të aplikuara të përpunimit, duke përfshirë ato automatike dhe manuale, që mbulojnë të gjitha proceset e veprimtarisë gjatë përpunimit të të dhënave personale;	5.1. Identification, assessment and treatment of major risks due to all applied forms of processing, including automatic and manual, covering all business processes during personal data processing;	5.1. Identifikaciju, procenu i tretman glavnih rizika zbog svih primenjenih oblika obrade, uključujući automatske i ručne, koji pokrivaju sve procese poslovanja tokom obrade ličnih podataka.
5.2. Trajtimi i të gjitha rreziqeve ligjore specifike për privatësinë dhe mbrojtjen e të dhënave.	5.2. Handling of all legal risks specific to privacy and data protection.	5.2. Rukovanje svim pravnim rizicima specifičnim za privatnost i zaštitu podataka.
Neni 19 **Dispozitat e veçanta për përpunimin manual**	**Article 19** **Special provisions for manual processing**	**Član 19** **Posebne odredbe ručne obrade**
1. Të gjitha dokumentet e përpunuara në mënyrë manuale të cilat përmbajnë të dhëna personale, përveq zbatimit të dispozitave nga Neni 12 i kësaj Rregullore, marrin masa shtesë për të parandaluar zbulimin e paligjshëm, shkatërrimin dhe humbjen, si në vend të punës ashtu edhe gjatë transferimit të tyre.	1. All manually processed documents containing personal data, except implementing the provisions of Article 12 of this Regulation, take additional measures in order to prevent unlawful disclosure, destruction and loss, both in the work place and while transferring thereof.	1. Sva ručno obrađena dokumenta, koja sadrže lične podatke, osim primene odredaba iz člana 12 ovog Pravilnika, uzimaju dodatne mere u cilju sprečavanja nezakonitog obelodanjivanja, uništavanja i gubitaka, kako na radnom mestu, tako i tokom prenosa istih.

2. SMSI duhet të përmbajë procedura specifike shtesë për të verifikuar se garancitë e tilla shtesë për trajtimin e dokumenteve në letër, në fakt zbatohen, dhe nëse përfshijnë të gjitha dokumentet gjatë gjithë ciklit të jetës të tyre, duke përfshirë edhe ato të krijuara përkohësisht, në veçanti dokumentet e printuara nga sistemet TIK.	2. The ISMS shall contain additional specific procedures to verify that such additional safeguards for handling paper documents are actually implemented, and that if they cover all documents all over their life cycle, including all those generated as temporary ones, in particular printouts from ICT systems.	2. SUBI sadrži dodatne specifične procedure za proveru da se takve dodatne mere za rukovanje papirnim dokumentima zapravo sprovode, i da li pokrivaju sva dokumenta širom njihovog životnog ciklusa, uključujući sva ona koja su izrađena kao privremena, odnosno ispise sa IKT sistema.
3. Në rastet kur dokumentet në letër krijohen si rezultate nga përpunimi i TIK-ut, qoftë si të përkohshme apo si ato përfundimtare zyrtare, printerët e përdorur për rezultate të tilla duhet të:	3. In case paper documents are created as outputs from ICT processing, either as temporary or as final official ones, the printers used for such output should be:	3. U slučaju da su papirni dokumenti kreirani kao izlazni rezultati iz obrade IKT-a, bilo kao privremeni ili kao konačni, štampači koji se koriste za takav izlaz treba da:
3.1. Administrohen në mënyrë qendrore;	3.1. Centrally administered;	3.1. Budu upravljani na centralnom nivou
3.2. Të kenë të aktivizuar tiparin e "shenjës ujore" (water mark) në mënyrë për të qenë në gjendje të gjurmohet çdo lëshues i një dokumenti të tillë të printuar.	3.2. Having activated their "water mark" capabilities in order to be able to trace each issuer of such a printed output.	3.2. Aktiviraju svoju sposobnost za "vodeni znak" kako bi mogli da prate svakog izdavača takvog štampanog izlaznog rezultata.
4. Nëse këto dokumente përmbajnë të dhëna të ndjeshme, atëherë duhet të zbatohen kontrolle shtesë në SMSI, sipas Nenit 6 të kësaj Rregullore.	4. If these documents contain sensitive data, additional controls shall be implemented in the ISMS, as in the Article 6 of this Regulation.	4. Ako ovi dokumenti sadrže osetljive podatke, treba sprovesti dodatne kontrole u SUBI-ju, prema članu 6 ovog Pravilnika.

Neni 20 Përpunimi i të dhënave të ndjeshme	Article 20 Processing of sensitive data	Član 20 obradu osetljivih podataka
1. Për subjektet që kryejnë përpunimin e të dhënave të ndjeshme në mënyrë manuale dhe automatike, pjesë kritike të sigurisë së procesimit duhet të identifikohen, veçanërisht lidhur me operacionet të tilla si:	1. For public and private bodies processing sensitive data both manually and automaticly, security critical parts of processing shall be identified, in particular concerning operations such as:	1. Za subjekte koji obrađuju osetljive podatke i ručno i automatski, svaki način obrade, Treba da se identifikuje posebno u vezi operacija kao što su:
1.1. Vënia e të dhënave në dispozicion;	1.1. Making data available;	1.1. Omogućavanje podataka dostupnim
1.2. Kopjimi;	1.2. Copying;	1.2. Kopiranje;
1.3. Arkivimi;	1.3. Archiving;	1.3. Arhiviranje;
1.4. Shkatërrimi;	1.4. Destructing;	1.4. Uništavanje;
1.5. Anonimizimi.	1.5. Anonymising;	1.5. Anonimizacija;
2. Në vazhdimësi të zbatimit të paragrafit 1 më lartë, duhet të bëhet kontrolli i dyfishtë për të gjitha pjesët e përpunimit në mënyrë që të parandalohet neglizhenca, gabimet njerëzore, shtrëngimi si dhe veprimtaria e synuar kriminale.	2. In the continuity of implementation of article 1 above, double checks shall be deployed to all these parts of processing in order to prevent against negligence, human error, coercing and an intended criminal activity.	2. Dupla provera treba biti urađena na svim ovim delovima obrade kako bi se sprečili nemar, ljudske greške, prinude i nameravane kriminalne aktivnosti.
3. Kujdes i veçantë shtesë do t'i kushtohet parandalimit të ndonjë zbulimi të paligjshëm:	3. Special additional attention shall be dedicated to preventing an unlawful disclosure:	3. Posebna dodatna pažnja biće posvećena sprečavanju nezakonitog otkrivanja:
3.1. në rast të përpunimit manual, SMSI	3.1. in case of manual processing, the	3.1. U slučaju ručne obrade, SUBI sadrži

duhet të përmbajë procedura specifike shtesë për trajtimin e dokumenteve të tilla në letër që përmbajnë këto të dhëna, në mënyrë që t'i parandalohet qasja personave të paautorizuar në të dhënat personale në këto dokumente gjatë gjithë ciklit të jetës së tyre.	ISMS shall contain additional specific procedures for handling such paper documents containing this data in order to prevent access of unauthorized persons to personal data contained in these documents all over their life cycle.	dodatne specifične procedure postupanja sa takvim papirnim dokumentima koji sadrže ove podatke u cilju sprečavanja pristupa neovlašćenih lica ličnim podacima sadržanim u ovim dokumentima širom njihovog životnog ciklusa.
3.2. Në rast të transferimit automatik të të dhënave personale të ndjeshme, rrugët e transmetimit apo dokumentet që përmbajnë këto të dhëna duhet koduar, duke përdorur mënyra dhe fuqi koduese në përputhje me rezultatin e vlerësimit të rreziqeve të kryer paraprakisht.	3.2. In case of automatic transfer of sensitive personal data, the transmission paths or the documents containing this data shall be encrypted, using encryption means and strengths in accordance with the outcome of the risks assessment carried out in advance.	3.2. U slučaju automatskog transfera prenosa osetljivih ličnih podataka, putevi prenosa ili dokumenti koji sadrže ove podatke treba da budu kodirani, korišćenjem sredstava i snaga za šifrovanje u skladu sa rezultatima procene rizika sprovedene unapred.
3.3. Përdorimi i mjeteve bartëse portative për të dhënat e tilla duhet të ndalohet në mënyrë eksplicite, përveç në rastet e kategorive të caktuara në situata emergjente, në të cilat duhet të merren masa shtesë, të tilla si:	3.3. Using portable media carriers for such data shall be explicitly banned, except in case of certain categories of emergency situations, in which additional measures shall be in place, such as:	3.3. Korišćenje prenosivih medijuma za takve podatke će biti izričito zabranjeno, osim u slučaju određenih kategorija vanrednih situacija, u kojima će dodatne mere biti na snazi, kao što su:
3.3.1. Verifikimi shtesë, që bartësi i të dhënave të jetë i koduar para se të vendosen të dhënat e ndjeshme në të;	3.3.1. Additional verification, that the data carrier was properly encrypted before putting any sensitive data on it;	3.3.1. Dodatne verifikacije da li je nosilac podataka pravilno kodiran pre stavljanja bilo kakvih osetljivih podataka na njega.
3.3.2. Verifikim shtesë, që më pas janë hequr me sukses të dhënat e ndjeshme në mënyrë të parevokueshme;	3.3.2. Additional verification, that the sensitive data was successfully removed afterwards in an irrevocable way;	3.3.2. Dodatne verifikacije da su osetljivi podaci uspešno uklonjeni nakon toga na nepovratan način.

3.3.3. Dokumentimi i çdo rasti të tillë të jashtëzakonshëm në dokumentacionin e situatave emergjente, në një mënyrë që do të mundëson identifikimin e kryesve të mundshëm, në rastin kur gabimi në respektimin e kësaj procedure do të rezultojë në zbulimin e paligjshëm.	3.3.3. Documenting each such an extraordinary case in the documentation of the emergency situations in a way which will make the possible perpetrators identifiable, in case when an error in observing this procedure would result in an unlawful disclosure.	3.3.3. Dokumentovanje svakog takvog vanrednog slučaja u dokumentaciji o vanrednim situacijama na način koji će omogućiti moguću identifikuju počinilaca, u slučaju kada će greška u posmatranju ovog postupka rezultirati nezakonitim otkrivanjem.
Neni 21 **Përpunimi portativ**	**Article 21** **Portable processing**	**Član 21** **Prenosiva obrada**
1. Në rast të përdorimit të mjeteve bartëse portative elektronike për të dhëna jo të ndieshme, duhet të enkriptohen para se të dalin nga ambientet e organit publik dhe privat të përpunimit.	1. In case of using portable electronic media for non-sensitive data as information carriers, they shall be encrypted before leaving premises of the public and private processing body.	1. U slučaju korišćenja prenosivih elektronskih medijuma kao nosilaca informacija, oni će biti enkriptirani pre napuštanja prostorije javnog i privatnog organa za obradu ličnih podataka.
2. Kjo dispozitë përfshinë të gjithë mjetet bartëse të tilla si:	2. This provision covers all media carriers such as:	2. Ova odredba pokriva sve nosioce medijuma kao što su:
2.1. Media Flash, CD, shiritat për regjistrim, dhe incizime të tjera.	2.1. Flash media, CD, tapes, and other recordings.	2.1. Fleš memorija, CD, trake i ostali snimci.
2.2. Të gjithë kompjuterët portativ në rast se ata janë të konfiguruar për të ruajtur të dhënat në ta, gjatë realizimit të përpunimit, veçanërisht të tilla si:	2.2. All portable computers in case they are configured to store data on them while conducting processing, in particular such as:	2.2. Svi prenosivi računari u slučaju da su konfigurisani za skladištenje podataka na njima pri obavljanu obrade, posebno kao što su:
2.2.1. Telefonat;	2.2.1. Phones;	2.2.1. Telefoni;

2.2.2. Telefonat e mençur; 2.2.3. Notebooks (kompjuter portativ), laptopët dhe lloje të tjera të kompjuterëve të vegjël; 2.2.4. Kompjuterit e dorës (palmtops). 3. Në rast të përdorimit të pajisjeve të tilla të lidhur me rrjetet publike: 3.1. Të gjitha rrugët e transmetimit duhet të përdorin mënyra të forta të enkriptimit. 3.2. Pajisjet duhet të administrohen nga qendra gjatë qasjes së tyre të parë në rrjetin publik, në mënyrë që në rast të humbjes, vjedhjes ose rënies së tyre nën kontroll të personave të paautorizuar, nga distanca të mund të: 3.2.1. Shkyçen; 3.2.2. Pastrohen të dhënat, edhe në rast se këto të dhëna janë mbajtur vetëm përkohësisht në to.	2.2.2. Smartphones; 2.2.3. Notebooks, laptops and sorts small computers; 2.2.4. Palmtops; 3. In case of using such devices as connected to public networks: 3.1. All transmission paths shall use strong encryption means. 3.2. Devices shall be centrally administered in a way allowing during their first access to public network, in case of their loss, theft or falling under control on unauthorised persons in another way, to be remotely: 3.2.1. Disabled; 3.2.2. Cleaned from data in case such had been even temporarily held on them.	2.2.2. Pametni telefoni 2.2.3. Notebook-ovi, laptopovi i sve vrste manjih računara 2.2.4. Palmtop-ovi 3. U slučaju korišćenja takvih uređaja dok su priključeni na javne mreže: 3.1. Svi putevi prenosa će koristiti jaka sredstva za enkriptiranje. 3.2. Uređaji se upravljaju na centralnom nivou na način koji dozvoljava, tokom njihovog prvog pristupa javnoj mreži, u slučaju njihovog gubitka, krađe ili padanja pod kontrolu neovlašćenog lica na drugi način, da budu daljinski: 3.2.1. Isključeni 3.2.2. Očišćeni od podataka u slučaju da su privremeno držani na njima.

Neni 22 **Dispozitat e veçanta për përdorim të "cloud computing"**	**Article 22** **Special provisions for "cloud computing" usage**	**Član 22** **Posebne odredbe tokom korišćenja "cloud computing"**
1. Në rast se organi publik dhe privat vendos të përpunojë pjesë të konsiderueshme të të dhënave të tyre personale duke përdorur Cloud Ccomputing, posaçërisht pjesën që përmbajnë të dhëna të ndjeshme, atëherë duhet të konsultohet Agjencia para angazhimit në një përpunimi të tillë.	1. In case the data processing public and private body decides to process a significant portion of its personal data by using Cloud Computing, especially its portion containing the sensitive data, Agency shall be consulted prior to engaging into such a processing.	1. U slučaju da javni i privatni organ za obradu podataka odluči da izvrši outsourcing za značajan deo svojih ličnih podataka, pogotovo onih koji sadrže osetljive podatke, Agencija će se ranije konsultovati pre angažovanja u takvoj obradi.
2. Agjencia ka të drejtë t'i lëshoj organit publik dhe privat udhëzime dhe udhëzues të veçantë, para se të lejohen të angazhohet në një aktivitet të tillë të procesimit të të dhënave.	2. Agency is allowed to issue separate instructions and guidelines for the public and private bodies, prior they are allowed to engage in such a data processing activity.	2. Agenciji je dozvoljeno da izda javnom i privatnom organu posebne instrukcije i smernice za subjekat, pre nego što je subjektu dozvoljeno da se bavi takvom aktivnošću.
Neni 23 **Vetëdijesimi i personelit për sigurinë e të dhënave**	**Article 23** **Data security awareness raising of personnel**	**Član 23** **Podizanje svesti osoblja o bezbednosti podataka**
1. Të gjithë përdoruesit, duke përfshirë personelin e vet si dhe atë të kontraktuar nga organi publik dhe privat, duhet të trajnohen rregullisht për sigurinë e mbrojtjes së të dhënave personale, në mënyrë që të mbahet një nivel i duhur i vetëdijes dhe respektimit të procedurave ekzistuese. Trajnimet duhet të kryhen në përputhje me afatet e	1. All users, including the personnel own and contracted by thepublic and private body, shall be trained regularly on personal data protection security in order to maintain a proper level of awareness and obedience of existing procedures. The trainings shall be performed according to the following schedules:	1. Svi korisnici, uključujući i sopstveno osoblje i angažovano od strane javnog i privatnog organasubjekta, preporučuje se da se redovno obučavaju za bezbednost zaštite ličnih podataka, kako bi se održao pravilan nivo svesti i poslušnosti postojećih procedura. Obuke će se obaviti u skladu sa sledećim rasporedom:

mëposhtme:		
1.1. Rregullisht, të paktën një herë në vit;	1.1. At least once a year on regular basis,	1.1. Najmanje jednom godišnje na redovnoj bazi;
1.1.1. Pas çdo amandamentimi substancial të ligjit të mbrojtjes së të dhënave personale në lidhje me sigurinë;	1.1.1. After every substantive amendment of the personal data protection law concerning security;	1.1.1. Nakon svake značajne izmene zakona za zaštitu ličnih podataka u vezi bezbednosti;
1.1.2. Pas çdo amandamentimi substancial të Kornizës ligjore Evropiane për mbrojtjen e të dhënave personale e cila publikohet paraprakisht në faqen zyrtare të Agjencisë - në rast se Organi publik dhe privat për përpunimin e të dhënave është i angazhuar në transferimet ndërkombëtare;	1.1.2. After every substantive amendment of the European legal Framework on personal data protection which is published in advance on the Agency's official website – in case the public and private body is engaged in international transfers.	1.1.2. Nakon svake značajne izmene Evropskog pravnog okvira o zaštiti ličnih podataka, koja je objavljena unapred na zvaničnom sajtu Agencije - u slučaju da javni i privatni organ za obradu podataka koji se bavi međunarodnim prenosima
1.1.3. Pas çdo ndryshimi substancial të SMSI-së, veçanërisht ndryshimet të PSI-së së saj;	1.1.3. After each substantial ISMS change, especially changes of its ISP;	1.1.3. Nakon svake suštinske promene SUBI-ja, naročito promene njenog PBI-ja;
1.1.4. Pas çdo ndryshimi substancial të procedurave të sigurisë për përpunimin e të dhënave personale ekzekutive në PSI në organin publik dhe privat për përpunim, apo në palën e tij të kontraktuar;	1.1.4. After each substantial change of personal data processing security procedures executive to the ISP at the public and private processingbody, or at its contracted party.	1.1.4. Nakon svake suštinske promene bezbednosnih postupaka obrade ličnih podataka izvršenih za PBI u javnom i privatnom organu za obradu, ili u ugovorenoj stranci;
1.1.5. Pas çdo shkelje të rëndë të	1.1.5. After each serious data security	1.1.1. Nakon svakog ozbiljnog

sigurisë së të dhënave, që rezulton në shkelje të ligjit për mbrojtjen e të dhënave - ajo që rezulton në dobësim serioz të besimit në aftësinë e përmbushjes së kushteve të sigurisë, dëmtimin e marrëdhënieve me publikun, dhe humbjet financiare.	breach resulting in violation of data protection law – the one resulting in a serious undermining of trust for being able to stay compliant in security terms, public relations damage, and financial loss.	kršenja bezbednosti podataka koje dovodi do povreda zakona o zaštiti ličnih podataka – onaj koji rezultira ozbiljnim podrivanjem poverenja što može da dovede do pogoršanja u bezbednosnom smislu, PR štete, i finansijskog gubitka.
2. Fushëveprimi i trajnimit dhe forma e tij organizative, duhet të zbatohet në përputhje me dispozitat e kësaj Rregullore, në përshtatshmëri me kërcënimet dhe dobësitë, rreziqet e identifikuara si dhe masave të urdhëruara për t'i zbutur ato.	2. The scope of training and its organisational form shall be applied in compliance with the provisions of this Regulation, in adequacy with identified threats and vulnerabilities, risks, and measures ordered to mitigate them.	2. Obim obuke i njen organizacioni oblik će se primenjivati u skladu sa odredbama ovog Uputstva, u adekvatnosti sa identifikovanim pretnjama i ranjivostima, rizicima i naloženim merama za ublažavanje istih.
3. Organi publik dhe privat duhet të siguroj trajnim profesional për zyrtarët e emëruar për mbrojtjen e të dhënave, ose personit tjetër të caktuar si përgjegjës për sigurinë e të dhënave personale, në rast se një zyrtar i tillë nuk është caktuar. Agjencia mund të kërkojë nga Organi publik dhe privat që të ofrojë dëshmi se trajnimi profesional në të vërtetë është mbajtur.	3. The public and private body shall ensure a professional training to the appointed Data Protection Officials or to the other appointed person in charge of personal security in case such an Official was not appointed. The Agency may request the public and private body to provide evidence that professional training actually took place.	3. Javni i privatni organ treba da obezbedi profesionalnu obuku imenovanim službenicima za zaštitu podataka, ili drugim imenovanim licima zaduženim za ličnu bezbednost u slučaju da takav službenik nije bio postavljen. Agencija može tražiti od javnog i privatnog organa da pruži dokaze da se je stručna obuka zaista održala.
Neni 24 **Rregullat për përmbushjen e sigurisë**	**Article 24** **Security Compliance Rules**	**Član 24** **Plavila usklađivanja bezbednosti**
1. Qasja formale e vlerësimit dhe analizës së rreziqeve të sigurisë së informacionit	1. Formal approach of information security risks analysis and assessment shall be	1. Formalan pristup analizi i proceni rizika bezbednosti informacija će biti

duhet të miratohet, dhe duhet të bazohet në standardet e sigurisë së informacionit të tilla si seria e standardeve ISO-27000 në mënyrë që t'i bëjnë mbrojtjen e të dhënave personale pjesë integrale të SMSI në kuadër të organit publik dhe privat. Preferohet, të përfshihen te gjitha informacionet e mbrojtura ligjërisht në sistemin e tillë, përveç informacionit sekret i cili ka mbrojtjen e tij të veçantë dhe kornizën e vlerësimit të pajtueshmërisë.	adopted, and it shall be based on the information security standards such as ISO-27000 series in order to make the personal data protection an integral part of the ISMS within thepublic and private body. It is preferable, to cover in such a system all legally protected information except classified information which has got its own separate protection and compliance assessment framework.	usvojen, a ona će se na osnovu standarda bezbednosti informacija, kao što su ISO-27000 serija kako bi zaštita ličnih podataka postala sastavni deo SUBI-ja u javnom i privatnom organu. Poželjno je da se u takvom sistemu pokriju sve zakonom zaštićene informacije osim tajnih podataka koji imaju svoju zasebnu zaštitu i usklađenost okvira procene.
1.1. Formësimi i SMSI sipas ISO-27002 është i detyrueshëm, siç është i përcaktuar me Nenin 18 të kësaj Rregullore.	1.1. Shaping the ISMS according to the ISO-27002 is mandatory, as set out by Article 18 of this Regulation.	1.1. Oblikovanje SUBI-ja prema ISO-27002 je obavezno, kao što je navedeno u članu 18 ovog Pravilnika.
1.2. Një raporti i jashtëm i azhurnuar i ISO-27001 i vlerësimit të përputhshmërisë se auditimit mund të pranohet nga Agjencia si dëshmi e përmbushjes së dispozitave për sigurinë e mbrojtjes së të dhënave personale nga organi publik dhe privat përpunues, vetëm nën kushtet e mëposhtme:	1.2. An up-to-date external ISO-27001 compliance audit assessment report can be fully accepted by the Agency as an evidence of processing public and private bodies compliance with the personal data protection security provisions, only under the following conditions:	1.2. Jedan ažurnirani eksterni revizorski izveštaj o proceni usklađenosti ISO-27001 može biti potpuno prihvaćen od strane Agencije kao dokaz o usklađenosti sa odredbama bezbednosti za zaštitu ličnih podataka od strane javnog i privatnog organa za obradu, samo pod sledećim uslovima:
1.2.1. Nëse organi publik dhe privat për përpunim dëshiron të përdorë raportin e tillë si dëshmi për përputhshmërinë e tij me ligjin për Mbrojtjen e të Dhënave Personale, sipas kërkesës.	1.2.1. If the processing public and private body wishes to use such a report as a proof for its compliance with the law on Protection of Personal Data, on its request.	1.2.1. Ukoliko javni i privatni organ za obradu želi da koristi takav izveštaj kao dokaz za njegovu usklađenost sa zakonom o zaštiti ličnih podataka, na njegov zahtev.

1.2.2. Raporti i tillë i vlerësimit konfirmon se certifikimi është ruajtur, dhe është vënë në dispozicion të Agjencisë.	1.2.2. Such an assessment report conforming that the certification is maintained,and is made available to the Agency.	1.2.2. Takav izveštaj o proceni koji potvrđuje da se sertifikacija održava, stavlja se na raspolaganje Agenciji.
1.3. Procesi i certifikimit përfshinë identifikimin, vlerësimin dhe zbutjen e kërcënimeve, dobësive dhe rreziqeve specifike të mbrojtjes së të dhënave personale, duke përfshirë çështjet ligjore.	1.3. The certification process covers identification, assessment and mitigation of personal data protection specific threats, vulnerabilities and risks, including the legal issues.	1.3. Proces sertifikacije pokriva identifikaciju, procenu i ublažavanje specifičnih pretnji, ranjivosti i rizika za zaštitu ličnih podataka, uključujući i pravna pitanja.
1.4. Agjencia kontrollon nëse:	1.4. The Agency checks then whether:	1.4. Agencija proverava da li je:
1.4.1. Perspektiva e të dhënave personale është përfshirë si duhet në matricën e kontrolleve dhe mjetet për zbutjen e rreziqeve janë adekuate dhe në fakt të zbatueshme në procesin e certifikimit;	1.4.1. The personal data perspective is properly included in the matrix of controls and the risks' mitigation means are adequate and actually implemented in the certification process;	1.4.1. Perspektiva ličnih podataka je pravilno uključena u matricu kontrola i sredstva za ublažavanje rizika su adekvatna i zapravo sprovedena u procesu sertifikacije.
1.4.2. Të gjitha proceset e veprimtarisë qe përfshijnë përpunimin e të dhënave personale përfshihen në procesin e certifikimit.	1.4.2. All the business processes involving personal data processing are included in the certification process.	1.4.2. Svi procesi poslovanja koji uključuju obradu ličnih podataka su uključeni u proces sertifikacije.
1.5. Nëse ky vlerësim i Agjencisë dëshmohet pozitiv, atëherë Agjencia, me kërkesën e organit publik dhe privat të certifikuar:	1.5. If this Agency's assessment proves positive, then Agency, on the request of the certified public and private body:	1.5. Ako procena ove agencije dokazuje pozitivno, onda Agencija, na zahtev sertifikovanog javnog i privatnog organa:

1.5.1. Mund të pranojë raportin e tillë të auditimit si dëshmi e pajtueshmërisë të sigurisë për mbrojtjen e të dhënave;	1.5.1. May accept such a audit's report as the data protection security's compliance proof	1.5.1. Može prihvatiti takvu reviziju izveštaja kao dokaz za usklađenost bezbednosti zaštite podataka.
1.5.2. Mund të lëshojë një njoftim të vlerësimit formal që do të shfaqet publikisht nga organi publik dhe privat si dëshmi e përmbushjes së sigurisë për të dhënat personale.	1.5.2. May issue a formal appraisal notification to be publicly displayed by the public and private body as its personal data security compliance proof.	1.5.2. Izdaje sopstveno formalno obaveštenje o proceni koje će biti javno prikazano od strane javnog i privatnog organa kao dokaz o usklađenosti bezbednosti ličnih podataka.
2. Para se të angazhohen në një marrëveshje kontraktuale, duke përfshirë përpunimin e të dhënave personale, organi publik dhe privat ka për detyrim të kontrolloj përputhshmërinë e përpunuesit me ligjin për Mbrojtjen e të Dhënave Personale.	2. Prior to engaging into a contractual agreement including personal data processing, the public and private body has the obligation to check processor's compliance with the law Protection of Personal Data.	2. Pre angažovanja u ugovornom sporazumu, uključujući obradu ličnih podataka, javni i privatni organ ima obavezu da proveri usklađenost obrađivača sa zakonom o zaštiti ličnih podataka.
2.1. Ky ekzaminim duhet gjithashtu të përfshijë inspektimin e lokaleve të palëve të kontraktuara, ku do te zhvillohet përpunimi aktual i të dhënave;	2.1. This examination shall also include inspecting the premises of the to be contracted party where the actual data processing is to be conducted;	2.1. Ovaj pregled obuhvata i kontrolu prostorija stranke koju treba ugovoriti gde stvarna obrada podataka treba da se obavlja.
2.2. Në rast se ky inspektim vendor nuk është i mundur ose është i pazbatueshëm, dhe rreziku që rezulton nga mos realizimi është vlerësuar si i pranueshëm, disa kontrolle ekuivalente shtesë duhet të përdoren nga organi publik dhe privat, veçanërisht gjatë kontraktimit te	2.2. In case this local inspection is not possible or impracticable, and the risk resulting from not doing this is assessed as being acceptable, some additional equivalent checks shall be used by thepublic and private body, especially while contracting the cloud-computing	2.2. U slučaju da ova lokalna inspekcija nije moguća ili nije praktična, a ako je rizik koji proizilazi, ako se ona ne uradi, ocenjen kao prihvatljiv, javni i privatni organ treba da koristi neke dodatne ekvivalente provere, pogotovo dok pri ugovaranju usluge obrade podataka

shërbimeve të përpunimit të të dhënave të bazuara në "cloud-computing" nga kompania e huaj.	based data processing services from a foreign company.	zasnovane na cloud-computingu iz inostrane kompanije.
Neni 25 **Njoftimi mbi shkeljen e të dhënave**	**Article 25** **Data breach notification**	**Član 25** **Obaveštenje o kršenju podataka**
1. Në rast të shkeljes së të dhënave personale, kontrolluesi duhet, pa vonesë, ta njoftojë Agjencinë për këtë shkelje të të dhënave personale. Njoftimi duhet të përshkruajë natyrën e shkeljes së të dhënave personale dhe pikat e kontaktit ku mund të merret më shumë informacion, pasojat dhe masat e propozuara ose të ndërmarra nga ofruesi për të adresuar shkeljen e të dhënave personale.	1. In the case of a personal data breach, the controller shall, without undue delay, notify the personal data breach to the Agency. The notification shall describe the nature of the personal data breach and the contact points where more information can be obtained, the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.	1. U slučaju kršenja ličnih podataka, kontrolor će, bez odlaganja, obavestiti Agenciju o kršenju ličnih podataka. Obaveštenje će opisati prirodu kršenja ličnih podataka i kontaktne tačke gde se mogu dobiti više informacija, posledice i predložene ili preduzete mere od strane provajdera za adresiranje kršenih ličnih podataka.
2. Agjencia, duke pasur parasysh efektet e mundshme negative të shkeljes, mund të kërkojë që kontrolluesit të njoftojë subjektet e të dhënave në lidhje me shkeljen e të dhënave personale.	2. The Agency, having considered the likely adverse effects of the breach, may require the controller to notify the data subjects about the personal data breach.	2. Agencija, nakon razmatranja mogućih negativnih efekata kršenja, može da zahteva da kontroler obavesti subjekte podataka o kršenju ličnih podataka.

KAPITULLI IV DISPOZITAT PËRFUNDIMTARE	CHAPTER IV FINAL PROVISIONS	POGLAVLJE IV ZAVRŠNE ODREDBE
Neni 26 **Përgjegjësia për mbikëqyrjen e sigurisë**	**Article 26** **Responsibility for supervision security**	**Član 26** **Odgovornost za nadzor bezbednosti**
1. Mbikëqyrja e sigurisë së mbrojtjes së të dhënave, sipas kësaj Rregullore është detyrë e Zyrtarit të Mbrojtjes së të Dhënave, ose personit tjetër të caktuar si përgjegjës për sigurinë e të dhënave personale.	1. Supervision of the data protection security according to this Regulation is duty of the Data Protection Official, or of another appointed person in charge of personal security.	1. Nadzor nad bezbednošću zaštite podataka prema ovom Administrativnom uputstvu je dužnost službenika za zaštitu podataka, ili drugog imenovanog lica zaduženog za bezbednost ličnih podataka .
2. Nëse gjatë inspektimit apo auditimit Agjencia gjen se organi publik apo privat ushtron veprimtari në kundërshtim me këtë Rregullore dhe me Nën-kreut B të ligjit mbi Mbrojtjen e të Dhënave Personale, Agjencia mund të shqiptoj kundërvajtje në përputhje me dispozitat e Kreut VII të ligjit mbi Mbrojtjen e të Dhënave Personale.	2. If during the inspection or audit Agency finds that public or private body carries out activities contrary to this Regulation and Sub-heading B of the Law on the Protection of Personal Data, the Agency may impose offense in conformity with the provisions of Chapter VII of the Law on the Protection of Personal Data.	2. Ukoliko u toku inspekcije ili revizije Agencija utvrdi da javni ili privatni organ obavlja delatnost suprotno ovim administrativnim uputstvom i podglavljem B Zakona o zaštiti ličnih podataka, Agencija može izreći prekršaj u skladu sa odredbama Poglavlja VII Zakona o Zaštiti ličnih podataka .
Neni 27 **Hyrja ne fuqi**	**Article 27** **Entry into force**	**Član 27** **Stupanje na snagu**
Kjo Rregullore hyn në fuqi 15 (pesëmbëdhjet) ditë pas nënshkrimit nga ana e Mbikëqyrësit Kryesor Shtetëror të ASHMDHP-së.	This regulation will be effective 15 (fifteen) days after signature by the Chief National Supervisor of NAPPD.	Ova uredba stupa na snagu 15 (petnaest) dana od potpisivanje od strane Glavnog Državnog Nadzornika Agencije.

Ruzhdi JASHARI Mbikëqyrës Kryesor Shtetëror 07 MAJ 2015	Ruzhdi JASHARI Chef National Supervisor 07 MAY 2015	Ruzhdi JASHARI Glavni Državni Nadzornik. 07 MAY 2015