# SKLEP KOMISIJE (EU) 2022/640

## z dne 7. aprila 2022

## o izvedbenih pravilih za vloge in odgovornosti glavnih varnostnih akterjev

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 249 Pogodbe,

ob upoštevanju Sklepa Komisije (EU, Euratom) 2015/443 z dne 13. marca 2015 o varnosti v Komisiji ([1]),

ob upoštevanju Sklepa Komisije (EU, Euratom) 2015/444 z dne 13. marca 2015 o varnostnih predpisih za varovanje tajnih podatkov EU ([2]),

ob upoštevanju naslednjega:

(1) Sklepa (EU, Euratom) 2015/443 in (EU, Euratom) 2015/444 se uporabljata za vse službe in prostore Komisije.

(2) Po potrebi se izvedbena pravila za dopolnitev Sklepa (EU, Euratom) 2015/444 ali v njegovo podporo sprejmejo v skladu s členom 60 Sklepa.

(3) Varnostni ukrepi za varovanje tajnih podatkov EU v celotnem življenjskem ciklu bi morali biti sorazmerni zlasti z njihovo stopnjo tajnosti.

(4) Varnostni ukrepi za varovanje komunikacijskih in informacijskih sistemov v Komisiji so določeni v Sklepu Komisije (EU, Euratom) 2017/46 ([3]), zlasti v členu 3 o načelih za varnost IT v Komisiji in členu 9 o lastnikih sistema.

(5) Namen izvedbenih pravil za vloge in odgovornosti glavnih varnostnih akterjev je določiti smernice o predpogojih in nalogah, ki so za te vloge določeni v sklepih (EU, Euratom) 2015/443 in (EU, Euratom) 2015/444.

(6) Člen 36(7) Sklepa (EU, Euratom) 2015/444 določa dodatne funkcije, povezane z varnostjo, ki jih prevzame varnostni organ Komisije. Naloge v zvezi s temi funkcijami so določene v tem sklepu.

(7) Lokalni uradniki za varnost in nadzorni uradniki registra imajo posebne odgovornosti za varovanje tajnih podatkov EU v svojih službah v skladu s Sklepom (EU, Euratom) 2015/444.

(8) Komisija je 4. maja 2016 sprejela sklep ([4]), ki člana Komisije, pristojnega za varnostne zadeve, pooblašča, da v imenu Komisije in na njeno odgovornost sprejme izvedbena pravila iz člena 60 Sklepa (EU, Euratom) 2015/444; 13. aprila 2021 je član Komisije, pristojen za varnostne zadeve, v imenu Komisije in na njeno odgovornost sprejel sklep ([5]), s katerim je pooblastila za ta izvedbena pravila nadalje prenesel na generalno direktorico Generalnega direktorata za človeške vire in varnost –

([1]) UL L 72, 17.3.2015, str. 41.
([2]) UL L 72, 17.3.2015, str. 53.
([3]) Sklep Komisije (EU, Euratom) 2017/46 z dne 10. januarja 2017 o varnosti komunikacijskih in informacijskih sistemov v Evropski komisiji (UL L 6, 11.1.2017, str. 40).
([4]) Sklep C(2016) 2797 final z dne 4. maja 2016 o pooblastitvi v zvezi z varnostjo.
([5]) Sklep C(2021) 2684 final z dne 13. aprila 2021 o nadaljnjem prenosu pooblastil, dodeljenih s Sklepom Komisije C(2016) 2797 o pooblastitvi v zvezi z varnostjo.

SPREJELA NASLEDNJI SKLEP:

POGLAVJE 1

## Splošne določbe

*Člen 1*

### Predmet urejanja in področje uporabe

1. Ta sklep določa vloge in odgovornosti glavnih varnostnih akterjev, ki so v skladu s sklepoma (EU, Euratom) 2015/443 in (EU, Euratom) 2015/444 odgovorni za varovanje tajnih podatkov EU v Komisiji.

2. Ta sklep se uporablja za vse službe Komisije in v vseh prostorih Komisije.

POGLAVJE 2

## Generalni direktorat za človeške vire in varnost

*Člen 2*

### Varnostni organ Komisije

1. Direktor Direktorata za varnost Generalnega direktorata za človeške vire in varnost je varnostni organ Komisije iz člena 7 Sklepa (EU, Euratom) 2015/444.

2. Varnostni organ Komisije v skladu s členoma 3 in 7 tega sklepa opravlja svoje funkcije na naslednjih področjih, kot so določena v Sklepu (EU, Euratom) 2015/444:

(a) varnost osebja;

(b) fizična varnost;

(c) upravljanje tajnih podatkov EU;

(d) akreditacija komunikacijskih in informacijskih sistemov za obravnavanje tajnih podatkov EU;

(e) industrijska varnost in

(f) izmenjava tajnih podatkov.

3. Varnostni organ Komisije poskrbi za obvezno usposabljanje lokalnih uradnikov za varnost, namestnikov lokalnih uradnikov za varnost, nadzornih uradnikov registra in namestnikov nadzornih uradnikov registra o njihovih odgovornostih in nalogah.

*Člen 3*

### Organ za zagotavljanje informacijske varnosti

Organ za zagotavljanje informacijske varnosti je odgovoren za naslednje dejavnosti v zvezi z varovanjem tajnih podatkov EU:

(a) razvijanje varnostnih politik in varnostnih smernic za zagotavljanje informacijske varnosti ter spremljanje njihove učinkovitosti in ustreznosti;

(b) varovanje in upravljanje tehničnih informacij, povezanih s šifrirnimi izdelki;

(c) zagotavljanje skladnosti ukrepov za zagotavljanje informacijske varnosti s politikami Komisije na področju varnosti in javnega naročanja, kot je ustrezno;

(d) zagotavljanje, da so šifrirni izdelki izbrani v skladu s politikami, ki določajo njihovo upravičenost in urejajo njihov izbor;

(e) posvetovanje z lastniki sistema, ponudniki sistema, varnostnimi akterji in predstavniki uporabnikov glede varnostnih politik in varnostnih smernic za zagotavljanje informacijske varnosti.

*Člen 4*

**Organ za varnostno akreditacijo**

1. Varnostni organ Komisije je odgovoren za akreditacijo varnostnih območij, ki izpolnjujejo zahteve iz člena 18 Sklepa 2015/444, ter komunikacijskih in informacijskih sistemov za obravnavanje tajnih podatkov EU.

2. Službe Komisije se v sodelovanju s svojim lokalnim uradnikom za varnost in svojim lokalnim varnostnim uradnikom za informatiko, kot je ustrezno, posvetujejo z organom za varnostno akreditacijo, kadar nameravajo:

(a) postaviti varnostno območje;

(b) vzpostaviti komunikacijski in informacijski sistem za obravnavanje tajnih podatkov EU;

(c) namestiti kakršno koli drugo opremo za obravnavanje tajnih podatkov, vključno s povezavami s komunikacijskimi in informacijskimi sistemi tretjih strani.

Organ za varnostno akreditacijo glede teh dejavnosti svetuje tako med načrtovanjem kot tudi med postavitvijo ali razvojem.

3. Tajni podatki EU se v varnostnem območju ali komunikacijskem in informacijskem sistemu ne obravnavajo, dokler organ za varnostno akreditacijo ne izda akreditacije na ustrezni stopnji tajnosti tajnih podatkov EU.

4. Zahteve za akreditacijo varnostnih območjih vključujejo:

(a) odobritev načrtov za varnostno območje;

(b) odobritev naročil del, ki jih izvedejo zunanji izvajalci, ob upoštevanju določb o industrijski varnosti, kot so zahteve za varnostna dovoljenja izvajalcev in njihovega osebja;

(c) razpoložljivost vseh potrebnih izjav in certifikatov o skladnosti;

(d) fizični inšpekcijski pregled varnostnega območja, s katerim se preveri, ali gradbeni materiali in metode, kontrole dostopa, varnostna oprema in vsi drugi predmeti izpolnjujejo zahteve, ki jih določi varnostni organ Komisije;

(e) potrditev protiukrepov proti elektromagnetnemu sevanju za vsa tehnično varovana območja;

(f) odobritev varnostno-operativnih postopkov za varnostno območje.

5. Zahteve za akreditacijo komunikacijskih in informacijskih sistemov za obravnavanje tajnih podatkov EU vključujejo:

(a) oblikovanje strategije za akreditacijo sistema;

(b) potrditev varnostnega načrta komunikacijskega in informacijskega sistema na podlagi pristopa obvladovanja tveganja;

(c) potrditev varnostno-operativnih postopkov za komunikacijski in informacijski sistem;

(d) potrditev vse druge zahtevane varnostne dokumentacije, kot jo določi organ za varnostno akreditacijo;

(e) odobritev vsakršne uporabe šifrirnih tehnologij;

(f) potrditev protiukrepov proti elektromagnetnemu sevanju za komunikacijski in informacijski sistem za obravnavanje podatkov stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali višje;

(g) inšpekcijski pregled komunikacijskega in informacijskega sistema, s katerim se preveri, ali se dokumentirani varnostni ukrepi pravilno izvajajo.

6. Po uspešni izpolnitvi zahtev za akreditacijo organ za varnostno akreditacijo izda uradno dovoljenje za obravnavanje tajnih podatkov EU v varnostnem območju ali komunikacijskem in informacijskem sistemu za navedeno najvišjo stopnjo tajnih podatkov EU in za največ pet let, odvisno od stopenj tajnosti obravnavanih tajnih podatkov EU in povezanih tveganj.

7. Ob uradnem obvestilu o kršitvi varovanja tajnosti ali znatni spremembi zasnove ali varnostnih ukrepov varnostnega območja ali komunikacijskega in informacijskega sistema organ za varnostno akreditacijo pregleda in po potrebi prekliče dovoljenje za obravnavanje tajnih podatkov EU, dokler ugotovljene težave niso odpravljene.

*Člen 5*

**Organ TEMPEST**

1. Varnostni ukrepi TEMPEST se izvajajo za zaščito komunikacijskega in informacijskega sistema za obravnavanje podatkov stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali višje ter se lahko izvajajo za podatke stopnje tajnosti RESTREINT UE/EU RESTRICTED.

2. Organ TEMPEST je odgovoren za odobritev ukrepov, sprejetih za varovanje pred nepooblaščenim razkritjem tajnih podatkov EU zaradi nenamernega elektromagnetnega oddajanja.

3. Organ TEMPEST na zahtevo lastnika komunikacijskega in informacijskega sistema za obravnavanje tajnih podatkov EU izda specifikacije za varnostne ukrepe TEMPEST glede na stopnjo tajnosti zadevnih podatkov.

4. Organ TEMPEST izvede tehnično preizkušanje med akreditacijo varnostnih območij ter komunikacijskih in informacijskih sistemov za obravnavanje tajnih podatkov EU na stopnji CONFIDENTIAL UE/EU CONFIDENTIAL ali višje ter po uspešnem preizkusu izda potrdilo TEMPEST.

5. V potrdilu TEMPEST se navedejo vsaj:

(a) datum preizkusa;

(b) opis varnostnih ukrepov TEMPEST z načrti prostorov;

(c) datum izteka veljavnosti potrdila;

(d) spremembe, ki razveljavijo potrdilo;

(e) podpis organa TEMPEST.

6. Lokalni uradnik za varnost ali organizator sestanka, pristojen za organizacijo zaupnih sestankov, v sodelovanju z lokalnim uradnikom za varnost lahko organ TEMPEST zaprosi za preizkus sejnih sob, da se zagotovi njihova tehnična varnost.

*Člen 6*

**Organ za odobritev šifrirnih metod in izdelkov**

1. Organ za odobritev šifrirnih metod in izdelkov je odgovoren za odobritev uporabe šifrirnih tehnologij.

2. Organ za odobritev šifrirnih metod in izdelkov izda smernice o zahtevah za uporabo in odobritev šifrirnih tehnologij.

3. Organ za odobritev šifrirnih metod in izdelkov odobri uporabo šifrirnih rešitev na podlagi zahtevka lastnika sistema. Odobritev se podeli na podlagi zadovoljive ocene vsaj:

(a) varnostnih potreb podatkov, ki jih je treba varovati;

(b) pregleda komunikacijskega in informacijskega sistema, vključenega v rešitev;

(c) ocene inherentnih in preostalih tveganj;

(d) opisa predlagane rešitve;

(e) varnostno-operativnih postopkov za šifrirno rešitev.

4. Organ za odobritev šifrirnih metod in izdelkov vodi register odobrenih šifrirnih rešitev.

*Člen 7*

**Organ za razpošiljanje šifrirnega materiala**

1. Organ za razpošiljanje šifrirnega materiala je odgovoren za razpošiljanje šifrirnega materiala, ki se uporablja za varovanje tajnih podatkov EU (predvsem šifrirne opreme, šifrirnih ključev, potrdil in povezanih avtentikatorjev), naslednjim prejemnikom:

(a) uporabnikom ali službam znotraj Komisije za komunikacijske in informacijske sisteme, ki jih upravljajo zunanje strani;

(b) uporabnikom ali organizacijam zunaj Komisije za komunikacijske in informacijske sisteme, ki jih upravlja Komisija.

2. Organ za razpošiljanje šifrirnega materiala lahko v skladu s členom 17(3) Sklepa 2015/443 odgovornost za razpošiljanje šifrirnega materiala tretjim stranem prenese na druge službe.

3. Organ za razpošiljanje šifrirnega materiala zagotovi, da se ves šifrirni material pošlje prek varnih kanalov, ki ščitijo pred vsakršnimi posegi oziroma jih dokazujejo, v skladu z varnostnimi predpisi, ki se uporabljajo za stopnjo tajnosti tajnih podatkov EU, ki jih bo ta material varoval.

4. Organ za razpošiljanje šifrirnega materiala zagotovi smernice lokalnemu uradniku za varnost, in kadar je primerno, lokalnemu varnostnemu uradniku za informatiko vsake službe Komisije, ki je vključena v pripravo, razpošiljanje ali uporabo šifrirnega materiala.

5. Organ za razpošiljanje šifrirnega materiala zagotovi, da se za razpošiljanje vzpostavijo ustrezni varnostno-operativni postopki.

POGLAVJE 3

**Službe Komisije**

*Člen 8*

**Vodje služb**

1. Vsak vodja službe imenuje:

(a) lokalnega uradnika za varnost in enega ali več namestnikov, kadar je to ustrezno, za svojo službo ali kabinet;

(b) nadzornega uradnika registra in enega ali več namestnikov, kadar je to ustrezno, za vsako službo, ki vodi register tajnih podatkov EU;

(c) lastnika sistema za vsak komunikacijski in informacijski sistem za obravnavanje tajnih podatkov EU.

2. Pred imenovanjem lokalnih uradnikov za varnost, namestnikov lokalnih uradnikov za varnost, nadzornih uradnikov registra in namestnikov nadzornih uradnikov registra vodja službe zaprosi za odobritev direktorja Direktorata za varnost Generalnega direktorata za človeške vire in varnost.

3. Vodja službe po posvetovanju z lokalnim uradnikom za varnost določi vsa delovna mesta, za katera je potrebno dovoljenje za dostop do tajnih podatkov EU. Kandidati za takšna delovna mesta se o zahtevi po dovoljenju obvestijo med postopkom zaposlovanja.

4. Vodja katere koli službe, ki ima tajne podatke EU, je odgovoren za aktiviranje načrtov za uničenje in evakuacijo v nujnih primerih, kadar je to potrebno. Načrti vključujejo nadomestno možnost za primere, ko ni mogoče stopiti v stik z vodjo službe.

*Člen 9*

**Lastniki komunikacijskih in informacijskih sistemov za obravnavanje tajnih podatkov EU**

1. Lastnik sistema čim bolj na začetku projekta za vzpostavitev komunikacijskega in informacijskega sistema za obravnavanje tajnih podatkov EU stopi v stik z organom za varnostno akreditacijo, da se določijo ustrezni varnostni standardi in zahteve ter začne postopek varnostne akreditacije.

2. Lastnik sistema zagotovi, da varnostni ukrepi izpolnjujejo zahteve organa za varnostno akreditacijo ter da komunikacijski in informacijski sistem pred pridobitvijo akreditacije ne obravnava tajnih podatkov EU.

3. Lastnik sistema za odobritev uporabe kakršne koli šifrirne tehnologije stopi v stik z organom za odobritev šifrirnih metod in izdelkov. Lastniki sistemov ne uporabljajo šifrirnih tehnologij v produkcijskih sistemih brez predhodne odobritve.

4. Za zadeve, povezane z varnostjo komunikacijskih in informacijskih sistemov, se lastnik sistema posvetuje z lokalnim varnostnim uradnikom za informatiko svoje službe.

5. Lastnik sistema najmanj enkrat letno pregleda varnostne ukrepe, ki se uporabljajo za sistem, vključno z njegovim varnostnim načrtom.

6. V primeru varnostnega incidenta v komunikacijskem in informacijskem sistemu, pri katerem je navedeno, da ta sistem ne more več ustrezno varovati tajnih podatkov EU, lastnik sistema o tem obvesti lokalnega uradnika za varnost ter nemudoma stopi v stik z organom za varnostno akreditacijo za nasvet o nadaljnjih korakih. V tem primeru se lahko akreditacija začasno prekliče in sistem izklopi, dokler se ne sprejmejo ustrezni korektivni ukrepi.

7. Lastnik sistema vselej v celoti podpira organ za varnostno akreditacijo pri njegovih nalogah v zvezi z akreditacijo komunikacijskega in informacijskega sistema.

*Člen 10*

**Operativni organ za zagotavljanje informacijske varnosti**

Operativni organ za zagotavljanje informacijske varnosti za vsak komunikacijski in informacijski sistem:

(a) pripravi varnostno dokumentacijo v skladu z varnostnimi politikami in smernicami, zlasti varnostni načrt, varnostno-operativne postopke, povezane s sistemom, in šifrirno dokumentacijo v okviru postopka akreditacije komunikacijskega in informacijskega sistema;

(b) sodeluje pri izboru in preizkušanju tehničnih varnostnih ukrepov, naprav in programske opreme, značilnih za sistem, zaradi nadzora nad njihovim izvajanjem in zagotovitve, da so varno nameščeni, konfigurirani in vzdrževani v skladu z ustrezno varnostno dokumentacijo;

(c) sodeluje pri izboru varnostnih ukrepov in naprav TEMPEST, če se zahtevajo v varnostnem načrtu, ter v sodelovanju z organom TEMPEST zagotovi, da so varno nameščeni in vzdrževani;

(d) nadzira izvajanje in uporabo varnostno-operativnih postopkov, povezanih z delovanjem sistema;

(e) upravlja šifrirne izdelke in ravna z njimi v sodelovanju z organom za razpošiljanje šifrirnega materiala, da zagotovi ustrezno hrambo šifrirnega materiala in nadzorovanega blaga ter po potrebi oblikovanje šifrirnih spremenljivk;

(f) izvaja varnostne analize, preglede in preizkuse, zlasti za pripravo ustreznih poročil o tveganju, ki jih zahteva organ za varnostno akreditacijo;

(g) poskrbi za posebno usposabljanje o zagotavljanju informacijske varnosti za komunikacijske in informacijske sisteme;

(h) izvaja in upravlja posebne varnostne ukrepe za komunikacijske in informacijske sisteme.

POGLAVJE 4

**Lokalni uradnik za varnost**

*Člen 11*

**Imenovanje lokalnega uradnika za varnost**

1. Lokalni uradnik za varnost in namestniki lokalnega uradnika za varnost so uradniki ali začasni uslužbenci.

2. Vsi lokalni uradniki za varnost in namestniki lokalnih uradnikov za varnost imajo veljavno pooblastilo za dostop do tajnih podatkov EU do stopnje tajnosti SECRET UE/EU SECRET in po potrebi do stopnje tajnosti TRES SECRET UE/EU TOP SECRET. Lokalni uradnik za varnost ali namestnik lokalnega uradnika za varnost pridobi pooblastilo za dostop do tajnih podatkov pred imenovanjem.

3. Predstavništva Komisije lahko varnostni organ Komisije zaprosijo za odobritev izjeme od zahtev iz odstavkov 1 in 2.

*Člen 12*

**Varnostno-operativni postopki za varnostna območja**

1. Lokalni uradnik za varnost zadevne službe Komisije pripravi varnostno-operativni postopek za vsako varnostno območje pod njegovo odgovornostjo.

2. Lokalni uradnik za varnost zagotovi, da varnostno-operativni postopki vključujejo naslednje zahteve:

(a) samo uslužbencem z veljavnim pooblastilom za dostop do tajnih podatkov in ugotovljeno potrebo po dostopu do dokumentov stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali višje se dovoli dostop brez spremstva v varnostno območje med delovnim časom;

(b) dostop brez spremstva v varnostno območje izven delovnega časa se dovoli samo lokalnemu uradniku za varnost zadevne službe, nadzornim uradnikom registra zadevnega varnostnega območja, njihovim namestnikom in pooblaščenemu osebju Direktorata za varnost Generalnega direktorata za človeške vire in varnost;

(c) snemalne in komunikacijske naprave, kot so mobilni telefoni, računalniki, fotoaparati ali druge pametne naprave, niso dovoljene v varnostnih območjih brez predhodnega dovoljenja varnostnega organa Komisije; za vsako odstopanje se vnaprej zaprosi varnostni organ Komisije; kontaktna točka je lokalni uradnik za varnost;

(d) vse notranje ali zunanje osebje, ki potrebuje dostop v varnostno območje, vendar ne izpolnjuje meril iz točke (a), pospremi in stalno nadzoruje ustrezno pooblaščen uslužbenec; vsak takšen dostop v varnostno območje se zabeleži v dnevniku, ki se hrani na vhodu v varnostno območje;

(e) lokalni uradnik za varnost zagotovi, da so sistemi za zaznavanje vdorov, ki nadzorujejo varnostno območje, ves čas aktivirani in pravilno delujejo, ter upravlja vsa povezana gesla, ključe, PIN-kode ali druge mehanizme za dostop in avtentikacijo;

(f) alarmi v varnostnem območju se sporočijo Direktoratu za varnost Generalnega direktorata za človeške vire in varnost, ki nemudoma obvesti lokalnega uradnika za varnost;

(g) lokalni uradnik za varnost službe, v kateri se nahaja varnostno območje, vodi evidenco vseh intervencij po alarmu ali varnostnem incidentu;

(h) vzpostavljeni so postopki za ukrepanje v primeru alarma ali drugih izrednih razmer v varnostnem območju, vključno z evakuacijo osebja ter zagotovitvijo hitrega odziva ekipe za izredne razmere v pristojnosti varnostnega organa Komisije in zunanjih služb za izredne razmere, kot je potrebno;

(i) lokalni uradnik za varnost o vsaki kršitvi varovanja tajnosti, ki se zgodi v varnostnem območju ali v povezavi z njim, nemudoma obvesti varnostni organ Komisije, da se določi ustrezen odziv;

(j) individualne pisarne, prostori in sefi znotraj varnostnega območja so zaklenjeni, kadar niso nadzorovani;

(k) osebje ne razpravlja o tajnih podatkih na hodnikih ali v drugih skupnih prostorih varnostnega območja, kadar so v bližini nepooblaščeni posamezniki.

*Člen 13*

**Varnostni ključi in kombinacije**

1. Lokalni uradnik za varnost je v celoti odgovoren za zagotavljanje ustreznega ravnanja s ključi in kombinacijami, ki se uporabljajo v varnostnih območjih ali za dostop v njih, ter njihove hrambe. Ključi in kombinacije se hranijo v blagajni in so zaščiteni najmanj na stopnji tajnosti gradiva, do katerega omogočajo dostop.

2. Lokalni uradnik za varnost vodi register blagajn in sob trezorjev ter posodobljen seznam vseh uslužbencev, ki imajo dostop do njih brez spremstva.

3. Lokalni uradnik za varnost vodi register ključev za blagajne in sobe trezorje, vključno z uslužbenci, katerim so dodeljeni. Za vsak izdani ključ se hrani potrdilo o prejemu, ki vključuje identifikacijo ključa, prejemnika, datum in uro.

4. Ključi in kombinacije se izdajo samo osebju, ki ima potrebo po seznanitvi in mu je bilo odobreno ustrezno pooblastilo za dostop do tajnih podatkov EU. Ko ti pogoji niso več izpolnjeni, lokalni uradnik za varnost pridobi ključ nazaj.

5. Lokalni uradnik za varnost hrani nadomestne ključe in pisne zapise vseh nastavitev kombinacij v posameznih zapečatenih, neprozornih, podpisanih in datiranih ovojnicah, ki jih zagotovijo uslužbenci, odgovorni za ključe. Te ovojnice se hranijo v blagajni, ki je namenjena za najvišjo stopnjo tajnosti gradiva, ki se hrani v zadevni blagajni ali sobi trezorju.

6. Če so ob spremembi kombinacije ali izmenjavi ključa na ovojnici vidne sledi posega ali poškodbe, lokalni uradnik za varnost to obravnava kot varnostni incident in nemudoma obvesti varnostni organ Komisije.

7. Spremembe nastavitev kombinacij blagajn v varnostnih območjih se izvajajo pod nadzorom lokalnega uradnika za varnost. Kombinacije se ponastavijo najmanj vsakih 12 mesecev ter:

(a) ob prejemu nove blagajne ali namestitvi nove ključavnice (zlasti je treba nemudoma spremeniti privzete kombinacije);

(b) ob sumu nepooblaščenega razkritja ali ob nepooblaščenem razkritju;

(c) kadar oseba, ki pozna kombinacijo, ne potrebuje več dostopa.

8. Lokalni uradnik za varnost vodi evidenco datumov sprememb kombinacij iz odstavka 7.

*Člen 14*

**Načrti za evakuacijo in uničenje tajnih podatkov EU v nujnih primerih**

1. Lokalni uradnik za varnost pomaga vodji službe pri pripravi načrtov za evakuacijo in uničenje tajnih podatkov EU v nujnih primerih na podlagi smernic Direktorata za varnost Generalnega direktorata za človeške vire in varnost.

2. Lokalni uradnik za varnost zagotovi, da je vsa oprema, potrebna za izvedbo načrtov iz odstavka 1, takoj na voljo in da se vzdržuje v dobrem stanju.

3. Lokalni uradnik za varnost skupaj z uradniki, imenovanimi v načrtih iz odstavka 1, najmanj vsakih 12 mesecev pregleda stanje pripravljenosti teh načrtov in sprejme vse potrebne ukrepe za njihovo posodobitev.

*Člen 15*

**Pooblastila za dostop do tajnih podatkov**

1. Lokalni uradnik za varnost vodi evidenco vseh delovnih mest znotraj službe, za katera je potrebno pooblastilo Komisije za dostop do tajnih podatkov, ter osebja, ki zaseda ta delovna mesta. Zahteva po pooblastilu za dostop do tajnih podatkov mora biti navedena v razpisu prostega delovnega mesta med postopkom zaposlovanja in kandidatu sporočena med razgovorom.

2. Lokalni uradnik za varnost nadzira vse zahtevke za pooblastila za dostop do tajnih podatkov EU. Lokalni uradnik za varnost je kontaktna točka znotraj službe in je glede pooblastil za dostop do tajnih podatkov v stiku z varnostnim organom Komisije.

3. Lokalni uradnik za varnost vloži zahtevek za začetek postopka za pridobitev pooblastila za dostop do tajnih podatkov v zvezi z zadevnim uslužbencem in zagotovi, da ta brez odlašanja varnostnemu organu Komisije vrne vprašalnik v zvezi z nacionalnim varnostnim preverjanjem.

4. Lokalni uradnik za varnost zagotovi, da se varnostno preverjeni uslužbenci njegove službe udeležijo obveznega seznanitvenega sestanka o tajnih podatkih EU za pridobitev pooblastila za dostop do tajnih podatkov.

5. Lokalni uradnik za varnost je v rednem stiku s službo za človeške vire svoje službe glede vseh sprememb na delovnih mest, za katera je potrebno pooblastilo za dostop do tajnih podatkov, ter o vsaki spremembi nemudoma obvesti varnostni organ Komisije.

6. Lokalni uradnik za varnost obvesti varnostni organ Komisije o prihodu novega uslužbenca, ki že ima dovoljenje za dostop do tajnih podatkov, na delovno mesto, ki ga mora zasedati varnostno preverjeni uslužbenec.

7. Lokalni uradnik za varnost zagotovi, da uslužbenci njegove službe v zahtevanem roku izpolnijo postopek za podaljšanje dovoljenja za dostop do tajnih podatkov. Uslužbenec, ki tega postopka ne želi izpolniti, bo premeščen na delovno mesto, za katerega ni potreben varnostno preverjeni uslužbenec.

*Člen 16*

**Register tajnih podatkov EU**

1. Kadar služba vodi register tajnih podatkov EU, lokalni uradnik za varnost nadzira dejavnosti nadzornih uradnikov registra v zvezi z obravnavanjem tajnih podatkov EU ter skladnost z varnostnimi predpisi za varovanje tajnih podatkov EU.

2. Lokalni uradnik za varnost najmanj vsakih 12 mesecev in ob zamenjavi nadzornega uradnika registra ali namestnika nadzornega uradnika registra izvede naslednje preglede:

(a) pregled vzorca dokumentov v registru tajnih podatkov EU za potrditev njihovega statusa in točnosti registra tajnih dokumentov;

(b) pregled vzorca potrdil o prejemu in potrdil o prenosu za pošiljanje tajnih podatkov EU v register tajnih podatkov EU in iz njega;

(c) pregled vzorca potrdil o uničenju.

3. Lokalni uradnik za varnost najmanj enkrat mesečno izvede naključni pregled registra tajnih dokumentov in nedavno prejetih tajnih dokumentov, da zagotovi pravilno evidentiranje dokumentov.

4. Vsi pregledi se zabeležijo v dnevniku registra tajnih dokumentov.

*Člen 17*

**Ostale odgovornosti glede varnosti**

Ostale odgovornosti glede varnosti lokalnega uradnika za varnost so določene v varnostnem obvestilu, ki zajema zlasti fizično varnost oseb, prostorov in drugih sredstev ter podatkov.

POGLAVJE 5

**Nadzorni uradnik registra**

*Člen 18*

**Imenovanje nadzornega uradnika registra**

1. Nadzorni uradnik registra in namestniki nadzornega uradnika registra so uradniki ali začasni uslužbenci.

2. Vsi nadzorni uradniki registra in namestniki nadzornih uradnikov registra imajo veljavno pooblastilo za dostop do tajnih podatkov EU do stopnje tajnosti SECRET UE/EU SECRET in po potrebi do stopnje tajnosti TRES SECRET UE/EU TOP SECRET. Nadzorni uradnik registra ali namestnik nadzornega uradnika registra pridobi pooblastilo za dostop do tajnih podatkov pred imenovanjem.

3. Predstavništva Komisije lahko varnostni organ Komisije zaprosijo za odobritev izjeme od zahtev iz odstavkov 1 in 2.

*Člen 19*

**Odgovornosti**

1. Nadzorni uradniki registra iz varnostnih razlogov vpišejo podatke stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, ko ti podatki:

(a) pridejo v službo Komisije ali gredo iz nje ali

(b) pridejo v komunikacijski in informacijski sistem ali gredo iz njega.

2. Nadzorni uradniki registra vpišejo vse dogodke v življenjskem ciklu vseh podatkov stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali višje. Nadzorni uradniki registra prav tako zagotovijo, da se vodi evidenca vseh podatkov stopnje tajnosti RESTREINT UE/EU RESTRICTED ali enakovrednih podatkov, ki se izmenjujejo s tretjimi državami in mednarodnimi organizacijami. To se izvaja v sodelovanju z registrom tajnih podatkov EU, ki ga upravlja generalni sekretariat.

3. Nadzorni uradnik registra dokumente stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali višje vpiše v register tajnih dokumentov ter zagotovi, da se varno hranijo v registru tajnih podatkov EU.

4. Nadzorni uradnik registra pomaga osebju Komisije pri ustvarjanju in pošiljanju podatkov stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali višje.

5. Kadar se prejmejo dokumenti stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali višje s strani drugih služb ali zunanjih strani, nadzorni uradnik registra zagotovi, da se zadevnemu tvorcu ustrezno vrne potrdilo o prejemu.

6. Preden se uslužbencu dovoli dostop do tajnega dokumenta iz registra tajnih podatkov EU, nadzorni uradnik registra pri lokalnem uradniku za varnost preveri, ali je varnostni organ Komisije tega uslužbenca varnostno preveril.

7. Nadzorni uradnik registra vpiše vse uslužbence, ki vstopijo v register tajnih podatkov EU in izstopijo iz njega ter niso pooblaščeni za dostop brez spremstva, in jih spremlja celotni čas obiska.

8. Kadar uslužbenec vzame dokument za vpogled zunaj registra tajnih podatkov EU, nadzorni uradnik registra zagotovi, da je ta uslužbenec seznanjen z ustreznimi izravnalnimi varnostnimi ukrepi in da dokument vrne takoj, ko ga ne potrebuje več. Nadzorni uradnik registra uslužbenca opozori, naj vsak tak dokument vrne čim prej.

9. Register tajnih podatkov EU izda kurirsko potrdilo, če se tajni dokumenti ročno odnesejo izven države, v kateri se nahaja register.

10. Podrobna navodila za nadzorne uradnike registra o vpisu tajnih dokumentov se navedejo v varnostnem obvestilu.

*Člen 20*

**Znižanje in preklic stopnje tajnosti**

Nadzorni uradnik registra službam, ki so podatke ustvarile, pomaga pri pregledovanju registriranih tajnih podatkov EU, da se ugotovi, ali je prvotna stopnja tajnosti še ustrezna oziroma ali se stopnja tajnosti dokumenta lahko zniža ali prekliče.

*Člen 21*

**Uničenje**

1. Nadzorni uradniki registra so odgovorni za uničenje podatkov stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL in višje z odobrenimi sredstvi, po potrebi v navzočnosti varnostno preverjenih prič.

2. Nadzorni uradniki registra evidentirajo vsako uničenje podatkov stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL in višje v registru tajnih dokumentov ter zadevna potrdila o uničenju hranijo v registru tajnih podatkov EU.

*Člen 22*

**Dodatne naloge**

1. Nadzorni uradnik registra lokalnemu uradniku za varnost nudi vso potrebno podporo pri njegovih nadzornih dejavnostih v registru tajnih podatkov EU.

2. Nadzorni uradnik registra o sumu varnostnih incidentov ali dejanskih varnostnih incidentih obvesti lokalnega uradnika za varnost, ki o njih obvesti varnostni organ Komisije.

3. Nadzorni uradnik registra tajnih podatkov EU službe Komisije, ki organizira sestanek stopnje tajnosti CONFIDENTIEL UE/EU CONFIDENTIAL ali višje, pripravi tajne podatke EU, ki se bodo obravnavali med sestankom, ter v sodelovanju z organizatorjem sestanka zagotovi, da se vsi dokumenti in potrdila obravnavajo v skladu z ustreznimi predpisi.

POGLAVJE 6

**Končne določbe**

*Člen 23*

**Preglednost**

O tem sklepu se obvesti osebje Komisije in vse osebe, za katere se uporablja, sklep pa se objavi v *Uradnem listu Evropske unije*.

*Člen 24*

Ta sklep začne veljati dan po objavi v *Uradnem listu Evropske unije*.

V Bruslju, 7. aprila 2022

*Za Komisijo*
*v imenu predsednice*
Gertrud INGESTAD
*generalna direktorica*
*Generalni direktorat za človeške vire in varnost*