

				Sem vložte název registrované právnické osoby							
Číslo dokumentu: PII06				Název dokumentu: Politika správy práv subjektů PII							
Verze: 1.0		Datum účinnosti: 01.01.2025		Vlastník dokumentu:							
X	Politika		Standard		Postup		Formulář		Registr		Jiné

Historie revizí				
Číslo revize	Datum revize	Změny	Přezkoumal	Vlastník procesu

Schválení			
Jméno	Funkce	Datum	Podpis

Právní upozornění (autorská práva a omezení užití)

(C) 2025 Clarysec LLC. All rights reserved.

Tento dokument je duševním vlastnictvím společnosti Clarysec LLC. Žádná jeho část nesmí být kopírována, znovu použita, distribuována ani upravována pro komerční nebo implementační účely bez výslovného písemného souhlasu.

Neoprávněné použití je přísně zakázáno a může vést k právním krokům.

V případě licencování kontaktujte: info@clarysec.com

V souladu s normami a právními předpisy

Norma / právní předpis	Kapitola / opatření / článek	Použitelnost	Typ pokrytí	Komentář
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Důkazy k žádostem o uplatnění práv a operativní řízení
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorování, neshody a nápravná opatření
ISO/IEC 27701:2025	Annex A.1.3.2	Controller	Primary	Povinnosti vůči subjektům PII
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7	Controller	Primary	Námítka, přístup, oprava a výmaz
ISO/IEC 27701:2025	Annex A.1.3.8; Annex A.1.3.9	Controller	Primary	Informování třetích stran a kopie zpracovávaných PII
ISO/IEC 27701:2025	Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Vyřizování žádostí a povinnosti související s automatizovaným rozhodováním
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Záznamy správce o zpracování
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Smlouva se zákazníkem, podpora povinností a záznamy zpracovatele
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Podpora zpracovatele pro povinnosti vůči subjektům PII
ISO/IEC 27701:2025	Annex A.3.14	Both	Supporting	Ochrana záznamů o žádostech o uplatnění práv
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Transparentnost a odpovědnost
GDPR	Article 11; Article 12	Controller	Primary	Identifikace, způsoby podávání žádostí, lhůty a správa odpovědí
GDPR	Article 15; Article 16; Article 17	Controller	Primary	Přístup, oprava a výmaz
GDPR	Article 18; Article 19; Article 20	Controller	Primary	Omezení zpracování,

				oznámení a přenositelnost
GDPR	Article 21; Article 22	Controller	Primary	Námítka a automatizované rozhodování
GDPR	Article 24	Controller	Supporting	Odpovědnost správce a opatření
GDPR	Article 26	Joint Controller	Supporting	Rozdělení odpovědností za práva u společných správců
GDPR	Article 28	Both	Primary	Součinnost zpracovatele při žádostech o uplatnění práv
GDPR	Article 30	Both	Supporting	Vazba na záznamy o zpracování
GDPR	Article 32	Both	Supporting	Bezpečné nakládání s důkazy o právech a zpřístupněními
GDPR	Article 39	Conditional	Supporting	Poradenství DPO a monitorování, kde se uplatní
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.12	Both	Supporting	Transparentnost, účast jednotlivce, odpovědnost a soulad
ISO/IEC 29151:2022	Annex A.10	Controller	Supporting	Účast subjektu PII a přístup

1. Rozsah

- 1.1 Tato politika stanoví povinné požadavky pro přijímání, validaci, posuzování, vyřizování, odmítání, prodlužování lhůt, uzavírání, monitorování a dokládání žádostí subjektů PII o uplatnění práv.
- 1.2 Tato politika se vztahuje na žádosti subjektů PII nebo oprávněných zástupců týkající se přístupu, opravy, výmazu, omezení zpracování, přenositelnosti, námitky, automatizovaného rozhodování, směřování odvolání souhlasu, stížností a souvisejících dotazů.
- 1.3 Tato politika se vztahuje na kontext správce, společného správce, zpracovatele a dílčího zpracovatele. Povinnosti zpracovatele a dílčího zpracovatele se uplatní pouze tehdy, když organizace podporuje správce, zákazníka nebo nadřazeného zpracovatele podle dokumentovaných pokynů.

1.4 Tato politika nenahrazuje:

- 1.4.1 PII03 pro evidenci činností zpracování a záznamy právního základu;
- 1.4.2 PII04 pro obsah a zveřejňování oznámení o ochraně osobních údajů;
- 1.4.3 PII05 pro plnění souhlasu a preferencí;
- 1.4.4 PII10 pro provádění uchovávání, mazání a likvidace;
- 1.4.5 PII11 pro správu a řízení přesnosti a kvality;
- 1.4.6 PII12 pro správu a řízení životního cyklu zpracovatele a dílčího zpracovatele;
- 1.4.7 PII15 pro zvládání incidentů a porušení zabezpečení.

2. Účel

- 2.1 Účelem této politiky je zajistit, aby žádosti subjektů PII o uplatnění práv byly vyřizovány konzistentně, zákonně, bezpečně, ve stanovených lhůtách a s důkazy připravenými pro audit.
- 2.2 Tato politika zajišťuje, aby organizace mohla prokázat odpovědnost za příjem žádostí, ověření totožnosti, posouzení, vyřízení, odmítnutí, prodloužení lhůty, spolupráci zpracovatele, uzavření a neustálé zlepšování.

3. Cíle

3.1 Cílem této politiky je:

- 3.1.1 Zajistit jednotný příjem a sledování všech žádostí subjektů PII o uplatnění práv.
- 3.1.2 Ověřit totožnost nebo oprávnění žadatele před zpřístupněním, opravou, výmazem, omezením zpracování nebo přenositelností.
- 3.1.3 Posuzovat žádosti vůči záznamům o zpracování, klasifikaci role, právním povinnostem, smluvním povinnostem a technické proveditelnosti.
- 3.1.4 Vyřizovat platné žádosti v dokumentovaných lhůtách.
- 3.1.5 Zaznamenávat důkazy o odmítnutí, částečném vyřízení, prodloužení lhůty a uzavření.
- 3.1.6 Podporovat povinnosti správce, pokud organizace jedná jako zpracovatel nebo dílčí zpracovatel.
- 3.1.7 Chránit záznamy o žádostech o uplatnění práv a balíčky odpovědí před neoprávněným zpřístupněním nebo změnou.
- 3.1.8 Monitorovat výkonnost vyřizování žádostí o uplatnění práv a podle potřeby prosazovat nápravná opatření.

4. Prohlášení politiky

4.1 Příjem, evidence a klasifikace

- 4.1.1 [All] Privacy Lead / PIMS Manager musí zaznamenat každou žádost subjektu PII o uplatnění práv do REG06 do dvou pracovních dnů od přijetí.

- 4.1.2 [All] Privacy Lead / PIMS Manager musí před zahájením posouzení klasifikovat v REG06 typ žádosti, kanál žádosti, datum žádosti, referenci totožnosti žadatele, přiřazeného vlastníka, interní termín splnění, zákonnou nebo smluvní lhůtu a aktuální stav.
- 4.1.3 [Controller] Privacy Lead / PIMS Manager musí potvrdit přijetí nebo poskytnout žadateli další požadovanou komunikaci do pěti pracovních dnů od přijetí a zaznamenat komunikaci v REG06.
- 4.1.4 [Controller] Process Owner / Business Owner musí propojit každou žádost s příslušnou činností zpracování v REG02 před přiřazením úkonů k vyřízení.
- 4.1.5 [Joint Controller] Privacy Lead / PIMS Manager musí před zahájením věcného posouzení identifikovat v REG02, REG06 nebo REG08 stranu společného správce odpovědnou za vyřízení žádosti.
- 4.1.6 [Processor] Privacy Lead / PIMS Manager musí před zahájením podpůrné činnosti zaznamenat každý pokyn zákazníka týkající se žádosti subjektu PII o uplatnění práv v REG06 a REG08.
- 4.1.7 [Subprocessor] Vendor / Procurement Owner musí před zahájením podpůrné činnosti dílčího zpracovatele zaznamenat každý nadřazený pokyn týkající se žádosti subjektu PII o uplatnění práv v REG06 nebo REG08.
- 4.1.8 [All] Incident Response Coordinator musí do jednoho pracovního dne zaznamenat eskalaci v REG10, pokud žádost o uplatnění práv naznačuje možný incident nebo porušení zabezpečení PII.

4.2 Ověření totožnosti, rozsah a posouzení

- 4.2.1 [Controller] Privacy Lead / PIMS Manager musí před zpřístupněním PII nebo provedením požadované změny ověřit totožnost žadatele nebo oprávnění zástupce v REG06.
- 4.2.2 [Controller] Privacy Lead / PIMS Manager musí požadovat pouze minimální dodatečné informace potřebné pro ověření a zaznamenat žádost v REG06, pokud totožnost nebo oprávnění nejsou dostatečné.
- 4.2.3 [Controller] Process Owner / Business Owner musí před posouzením vyřízení identifikovat z REG02 relevantní systémy, záznamy, účely, kategorie PII, příjemce a omezení uchovávání.
- 4.2.4 [Controller] Data Protection Officer / Privacy Advisor musí před sdělením rozhodnutí přezkoumat v REG06 vysoce rizikové, sporné, nejasné, nadměrné, opakované, odmítnuté nebo částečně vyřízené žádosti.
- 4.2.5 [Controller] System Owner / Application Owner musí před uvolněním balíčku odpovědi ověřit, že navržené výpisy odpovědi neobsahují nesouvisející PII ani neoprávněné údaje třetích stran.
- 4.2.6 [Controller] Information Security Lead musí před zpřístupněním velkého objemu PII, citlivých PII, zvláštních kategorií PII nebo vysoce rizikových PII přezkoumat způsob doručení odpovědi v REG06 nebo REG12.
- 4.2.7 [Controller] Data Protection Officer / Privacy Advisor musí před vyřízením, odmítnutím nebo eskalací přezkoumat v REG06 a REG04 žádosti související s automatizovaným rozhodováním nebo profilováním.
- 4.2.8 [Both] Privacy Lead / PIMS Manager musí před vyřízením nebo odmítnutím zaznamenat v REG06 výsledek posouzení, použitelný typ žádosti, rozhodnutí, odůvodnění a další krok.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Výjimky

- 9.1.1 [All] Process Owner / Business Owner musí před odchýlením se od schválených požadavků na příjem, ověření, vyřízení, odpověď nebo uzavření práv požádat o výjimku v REG12.
- 9.1.2 [All] Privacy Lead / PIMS Manager musí před implementací schválit nebo zamítnout každou výjimku při vyřizování práv v REG12.
- 9.1.3 [Controller] Data Protection Officer / Privacy Advisor musí před schválením přezkoumat každou výjimku zahrnující odmítnutí, částečné vyřízení, nejistotu totožnosti, citlivé PII, automatizované rozhodování, žádosti související s dětmi nebo vysoce rizikové zpracování.
- 9.1.4 [Both] System Owner / Application Owner musí zablokovat zpřístupnění, opravu, výmaz, omezení nebo export, pokud požadovaná výjimka nebyla před úkonem schválena v REG12.
- 9.1.5 [All] Privacy Lead / PIMS Manager musí každé schválené výjimce při vyřizování práv před její aktivací přiřadit v REG12 datum skončení platnosti, vlastníka a kompenzační opatření.

10. Prosazování požadavků politiky

- 10.1.1 [All] Privacy Lead / PIMS Manager musí do pěti pracovních dnů od zjištění opožděného, chybějícího, neúplného, neověřeného nebo nepodloženého záznamu žádosti o uplatnění práv zaznamenat neshodu v REG12.
- 10.1.2 [Controller] System Owner / Application Owner musí pozastavit zpřístupnění odpovědi, dokud nejsou v REG06 zaznamenány kontroly totožnosti, oprávnění a balíčku odpovědi.
- 10.1.3 [Both] Vendor / Procurement Owner musí do pěti pracovních dnů od zjištění eskalovat nespolupráci zpracovatele, dílčího zpracovatele nebo třetí strany v REG08 a REG12.
- 10.1.4 [All] Top Management musí při systémových, opakovaných nebo pro certifikaci relevantních selháních žádostí o uplatnění práv přiřadit vlastnictví nápravného opatření v REG12.
- 10.1.5 [All] Internal Audit / Compliance Reviewer musí do přiřazeného termínu splnění ověřit důkazy o uzavření nápravných opatření souvisejících s právy v REG12.
- 10.1.6 [All] Incident Response Coordinator musí do jednoho pracovního dne zahájit přezkum REG10, pokud neshoda žádosti o uplatnění práv naznačuje neoprávněné zpřístupnění, ztrátu, změnu, nedostupnost nebo jiný podezřelý incident PII.

11. Přezkum a údržba

- 11.1.1 [All] Privacy Lead / PIMS Manager musí tuto politiku každoročně přezkoumat a zaznamenat výsledek přezkumu v REG12.
- 11.1.2 [All] Privacy Lead / PIMS Manager musí tuto politiku přezkoumat do 30 dnů od významné změny práva týkajícího se žádostí o uplatnění práv, rozsahu činností zpracování, nástrojů pro práva, metody ověřování totožnosti, servisního modelu zpracovatele nebo požadavků certifikace PIMS.
- 11.1.3 [All] Data Protection Officer / Privacy Advisor musí před schválením přezkoumat v REG12 změny této politiky významné z hlediska ochrany osobních údajů.
- 11.1.4 [All] Top Management musí před zveřejněním schválit významné změny této politiky v REG12.
- 11.1.5 [All] Privacy Lead / PIMS Manager musí do 30 dnů od zveřejnění zaznamenat v REG11 komunikaci schválených změn politiky.

12. Související politiky

- 12.1 Tuto politiku podporují následující související politiky:
- 12.2 PII01 - Politika systému řízení informací o soukromí
- 12.3 PII02 - Politika rolí, odpovědností a odpovědnosti za ochranu soukromí

- 12.4 PII03 - Politika evidence zpracování PII a právního základu
- 12.5 PII04 - Politika oznámení o ochraně osobních údajů a transparentnosti
- 12.6 PII05 - Politika správy souhlasů a preferencí
- 12.7 PII07 - Politika posouzení rizik pro soukromí a DPIA
- 12.8 PII08 - Politika ochrany soukromí již od návrhu a ve výchozím nastavení
- 12.9 PII09 - Politika shromažďování, používání, zpřístupňování a sdílení PII
- 12.10 PII10 - Politika uchovávání, mazání a likvidace PII
- 12.11 PII11 - Politika přesnosti a kvality PII
- 12.12 PII12 - Politika správy soukromí pro zpracovatele, dílčí zpracovatele a třetí strany
- 12.13 PII13 - Politika mezinárodních přenosů PII
- 12.14 PII14 - Politika zabezpečení PII a řízení přístupu
- 12.15 PII15 - Politika řízení incidentů a porušení zabezpečení PII
- 12.16 PII16 - Politika školení, povědomí a kompetencí v oblasti ochrany soukromí
- 12.17 PII17 - Politika dokumentovaných informací a správy důkazů PIMS
- 12.18 PII18 - Politika monitorování, auditu a zlepšování PIMS

13. Referenční normy a rámce

- 13.1 Tato politika je mapována na následující normy a právní předpisy. Mapování vysvětluje, jak politika podporuje citované požadavky, a identifikuje interní ustanovení, která je implementují nebo podporují.

13.2 ISO/IEC 27701:2025

- 13.2.1 **Clause 7.5; Clause 8.1** - Mapováno na dokumentované záznamy žádostí o uplatnění práv, provozní pracovní postup žádostí, ověření totožnosti, vyřízení, odpověď, uzavření a důkazy o podpoře zpracovatele. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.8; 4.3.10; 4.4.5; 7.1.1; 7.1.2; 7.1.3].
- 13.2.2 **Clause 9.1; Clause 10.2** - Mapováno na metriky žádostí o uplatnění práv, monitorování opožděných žádostí, auditní vzorkování, zaznamenávání neshod, nápravná opatření a ověřování účinnosti. Addressed by clauses [4.5.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 10.1.1; 10.1.3; 10.1.4; 10.1.5].
- 13.2.3 **Annex A.1.3.2** - Mapováno na určování a plnění povinností vůči subjektům PII prostřednictvím dokumentovaných kategorií práv, kanálů příjmu, ověření, posouzení, odpovědi a kritérií uzavření. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.8; 4.4.1; 4.4.4; 6.1.1; 7.1.1].
- 13.2.4 **Annex A.1.3.6; Annex A.1.3.7** - Mapováno na námitku, přístup, opravu, výmaz, vyřizování omezení zpracování, ověření, vyřízení a řešení sporů o přesnost. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.6; 4.4.6].
- 13.2.5 **Annex A.1.3.8; Annex A.1.3.9** - Mapováno na informování třetích stran po výsledcích práv a poskytování kopií nebo přenositelných balíčků odpovědi. Addressed by clauses [4.3.5; 4.3.8; 4.5.5].
- 13.2.6 **Annex A.1.3.10; Annex A.1.3.11** - Mapováno na dokumentované vyřizování oprávněných žádostí, lhůty, prodloužení, odmítnutí, uzavření a přezkum žádostí souvisejících s automatizovaným rozhodováním. Addressed by clauses [4.1.2; 4.2.4; 4.2.7; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].
- 13.2.7 **Annex A.1.2.9** - Mapováno na propojení žádostí o uplatnění práv se záznamy o zpracování, účely zpracování, systémy, kategoriemi, příjemci a omezeními uchovávání. Addressed by clauses [4.1.4; 4.2.3; 4.3.8; 7.1.3].

- 13.2.8 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Mapováno na pokyny ze smlouvy se zákazníkem, podporu zpracovatele pro povinnosti zákazníka a záznamy zpracovatele pro činnosti podpory práv. Addressed by clauses [4.1.6; 4.1.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 7.1.7].
- 13.2.9 **Annex A.2.3.2** - Mapováno na prostředky zpracovatele pro podporu povinností správce vůči subjektům PII, včetně podpory vyhledání, opravy, omezení, výmazu a exportu podle dokumentovaného pokynu. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.1.7].
- 13.2.10 **Annex A.3.14** - Mapováno na ochranu záznamů o žádostech o uplatnění práv, bezpečné nakládání s balíčky odpovědí, kontroly doručení odpovědi a ochranu důkazů o uzavření. Addressed by clauses [4.2.5; 4.2.6; 4.4.5; 4.4.7; 7.1.4; 7.1.5; 10.1.2].

13.3 GDPR

- 13.3.1 **Article 5(1)(a); Article 5(2)** - Mapováno na transparentní vyřizování práv, důkazy o odpovědnosti, logy žádostí, záznamy odpovědí, auditní vzorkování a nápravná opatření. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.4; 4.4.5; 8.1.5; 10.1.1].
- 13.3.2 **Article 11; Article 12** - Mapováno na identifikaci, dodatečné informace, pokud jsou nezbytné, načasování odpovědi, komunikaci, prodloužení, odmítnutí a uzavření žádosti. Addressed by clauses [4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].
- 13.3.3 **Article 15; Article 16; Article 17** - Mapováno na výsledky vyhledání pro přístup, opravu, výmaz, ověření, důkazy o vyřízení a doručení balíčku odpovědi. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.3.10].
- 13.3.4 **Article 18; Article 19; Article 20** - Mapováno na omezení zpracování, oznámení výsledků práv relevantním stranám a přenositelnost nebo doručení kopie. Addressed by clauses [4.3.4; 4.3.5; 4.3.8; 4.5.5].
- 13.3.5 **Article 21; Article 22** - Mapováno na posouzení námitky a přezkum žádosti související s automatizovaným rozhodováním nebo profilováním. Addressed by clauses [4.2.7; 4.3.6; 4.3.7].
- 13.3.6 **Article 24** - Mapováno na opatření správy a řízení správce, role, vlastnictví pracovního postupu, přezkum, výjimky, nápravná opatření a dohled vedení nad vyřizováním práv. Addressed by clauses [5.1.1; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 9.1.1; 9.1.2; 10.1.4; 11.1.1].
- 13.3.7 **Article 26** - Mapováno na určení odpovědnosti společného správce za vyřizování žádostí před zahájením věcného posouzení. Addressed by clauses [4.1.5; 6.1.5].
- 13.3.8 **Article 28** - Mapováno na součinnost zpracovatele a dílčího zpracovatele, dokumentované pokyny zákazníka, lhůty podpory, zákaz přímé odpovědi bez autorizace a eskalaci nespolupráce. Addressed by clauses [4.1.6; 4.1.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.6; 6.1.6].
- 13.3.9 **Article 30** - Mapováno na propojení žádostí o uplatnění práv se záznamy o zpracování, činnostmi zpracování, systémy, kategoriemi PII, příjemci a záznamy zpracovatele. Addressed by clauses [4.1.4; 4.2.3; 4.3.8; 4.5.1; 7.1.3].
- 13.3.10 **Article 32** - Mapováno na bezpečné vyřizování žádostí o uplatnění práv, ochranu doručení odpovědi, prevenci neoprávněného zpřístupnění a ochranu důkazů o právech. Addressed by clauses [4.2.5; 4.2.6; 7.1.4; 7.1.5; 10.1.2; 10.1.6].
- 13.3.11 **Article 39** - Mapováno na poradenství a monitorování ze strany Data Protection Officer / Privacy Advisor pro vysoce rizikové, sporné, odmítnuté, prodloužené a s automatizovaným rozhodováním související žádosti o uplatnění práv. Addressed by clauses [4.2.4; 4.2.7; 4.3.7; 4.4.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

- 13.4.1 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.12** - Mapováno na transparentnost kanálů pro uplatnění práv, účast jednotlivce a přístup, odpovědnost, postupy pro stížnosti a nápravu,

monitorování souladu v oblasti ochrany soukromí a auditní důkazy. Addressed by clauses [4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.8; 4.4.6; 7.1.1; 8.1.5; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.10** - Mapováno na účast a přístup subjektu PII, ověření totožnosti, přístup, opravu, výmaz, aktualizace stavu, podporu zpracovatele a mechanismy pro stížnosti a nápravu. Addressed by clauses [4.1.1; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.4; 4.5.1; 4.5.4; 8.1.6].

13.6 Interní požadavky

13.6.1 Interní požadavek - Ustanovení definující REG06 jako primární evidenční objekt důkazů o právech, školení, schvalování nestandardních pracovních postupů, datum skončení platnosti výjimek, přezkum politiky a komunikaci změn politiky podporují konzistentní implementaci, ale nejsou přímo mapována na jedno externí ustanovení. Addressed by clauses [5.1.2; 6.1.7; 7.1.6; 9.1.4; 9.1.5; 11.1.2; 11.1.4; 11.1.5].