

				Sem vložte název registrované právnické osoby							
Číslo dokumentu: PII22				Název dokumentu: Politika ochrany soukromí v marketingu a používání cookies							
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

<p>Právní upozornění (autorská práva a omezení užití) (C) 2025 Clarysec LLC. All rights reserved.</p> <p>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.</p> <p>Neoprávněné použití je přísně zakázáno a může vést k právním krokům.</p> <p>V případě licencování kontaktujte: info@clarysec.com</p>
--

V souladu s normami a právními předpisy

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumentované důkazy o ochraně soukromí v marketingu 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.1.2.2; Annex A.1.2.3; Annex A.1.2.4; Annex A.1.2.5; Annex A.1.2.9	Controller	Primary	Marketingové účely, vazba na právní základ, souhlas a záznamy o zpracování
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Marketingoví zpracovatelé a odpovědnosti společných správců
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4; Annex A.1.3.5	Controller	Primary	Marketingová oznámení, oznámení o cookies a informace o odvolání souhlasu
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.10	Controller	Supporting	Směrování námitek a vyřizování žádostí pro přímý marketing
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Shromažďování, zpracování a minimalizace pro marketing a sledování
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5	Conditional	Supporting	Směrování předávání a zpřístupňování pro adtech a analytiku
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Smlouva se zpracovatelem, pokyny, zákaznická podpora a záznamy zpracovatele

ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Podpora zpracovatele pro povinnosti a směřování předávání a zpřístupňování
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Ochrana záznamů a důkazů z protokolování pro sledování změn
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Primary	Korektnost, transparentnost, omezení účelu, minimalizace a odpovědnost
GDPR	Article 6; Article 7	Controller	Primary	Zákonnost a podmínky souhlasu
GDPR	Article 12; Article 13; Article 14	Controller	Primary	Transparentní informace a oznámení
GDPR	Article 21	Controller	Primary	Námítka proti přímému marketingu a směřování odhlášení
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32	Both	Supporting	Odpovědnost, ochrana osobních údajů již od návrhu a ve výchozím nastavení, společní správci, zpracovatelé, záznamy a podpora zabezpečení
GDPR	Article 44	Conditional	Referenced	Směřování mezinárodního předávání pro marketingové dodavatele
ISO/IEC 29100:2020	Clause 5.1; Clause 5.8; Clause 5.9	Both	Primary	Souhlas a volba, transparentnost a účast
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Účel, shromažďování, minimalizace a omezení použití a zpřístupnění

ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Odpovědnost, bezpečnost informací a soulad
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Souhlas, účel, shromažďování, minimalizace, použití/zpřístupnění a opatření účasti
ISO/IEC TS 27560:2023	Clause 5.2; Clause 5.3; Clause 6.2; Clause 6.4	Controller	Supporting	Struktura záznamu o souhlasu a potvrzení o souhlasu, je-li používána

1. Rozsah

1.1 Tato politika stanoví povinné požadavky na ochranu soukromí pro marketing, cookies, sledovací technologie, analytiku, reklamní technologie, segmentaci publika, přímý marketing, správu preferencí, supresi, tagy třetích stran, přezkum kampaní a související zpracování PII.

1.2 Tato politika se vztahuje na kontexty správce, společného správce, zpracovatele a dílčího zpracovatele. Povinnosti správce platí tam, kde organizace určuje marketingové účely a prostředky. Povinnosti zpracovatele a dílčího zpracovatele platí pouze tam, kde organizace zpracovává marketingové, analytické, sledovací nebo kampaňové PII na základě dokumentovaných pokynů zákazníka nebo nadřazeného zpracovatele.

1.3 Tato politika zahrnuje:

- 1.3.1 evidenci činností marketingového zpracování a vazbu na účel;
- 1.3.2 důkazy o souhlasu a preferencích pro marketing a sledování;
- 1.3.3 správu cookies, sledovacích technologií a tagů;
- 1.3.4 záznamy oznámení o ochraně osobních údajů pro marketing a oznámení o cookies;
- 1.3.5 směřování suprese, odvolání souhlasu a odhlášení;
- 1.3.6 správu vztahů s marketingovými dodavateli, poskytovateli analytiky a adtech;
- 1.3.7 směřování mezinárodního předávání pro marketingové dodavatele a platformy;
- 1.3.8 důkazy o přezkumu a monitorování kampaní.

1.4 Tato politika nevytváří samostatný registr cookies, registr tagů, registr suprese, registr marketingových kampaní, registr analytiky, pracovní postup právního poradenství, výbor, řídicí panel, formulář ani nekanonickou roli.

1.5 Tato politika nenahrazuje:

- 1.5.1 PII03 pro evidenci činností zpracování a vlastnictví právního základu;
- 1.5.2 PII04 pro obecnou správu oznámení o ochraně osobních údajů;
- 1.5.3 PII05 pro souhlas a správu preferencí;
- 1.5.4 PII06 pro pracovní postup žádostí subjektů PII o uplatnění práv;
- 1.5.5 PII07 pro metodiku posouzení rizik pro soukromí a DPIA;
- 1.5.6 PII08 pro kontrolní body ochrany soukromí již od návrhu a ve výchozím nastavení;
- 1.5.7 PII09 pro obecná opatření pro shromažďování, použití, zpřístupňování a sdílení;
- 1.5.8 PII10 pro provádění uchovávání, výmazu a likvidace;
- 1.5.9 PII11 pro správu přesnosti a kvality;
- 1.5.10 PII12 pro správu životního cyklu zpracovatelů, dílčích zpracovatelů a třetích stran;
- 1.5.11 PII13 pro posouzení mechanismu mezinárodního předávání;
- 1.5.12 PII14 pro bezpečnost PII a architekturu řízení přístupu;
- 1.5.13 PII15 pro zvládání incidentů a porušení zabezpečení týkajících se PII;
- 1.5.14 PII18 pro správu monitorování, auditu a zlepšování PIMS;
- 1.5.15 PII20 pro ochranná opatření při marketingu nebo sledování specificky zaměřeném na děti;
- 1.5.16 PII21 pro opatření ochrany soukromí u AI, profilování a automatizovaného rozhodování;
- 1.5.17 PII23 pro opatření cloudového zpracovatele PII, kde se použijí.

2. Účel

2.1 Účelem této politiky je zajistit, aby marketing, cookies, analytika, sledování a zpracování v oblasti adtech byly řízeny prostřednictvím jasných záznamů účelů, transparentních oznámení, odpovídajících opatření pro souhlas nebo preference, zpracování suprese a odvolání, dohledu nad třetími stranami a důkazů připravených pro audit.

2.2 Tato politika podporuje odpovědnost za ochranu soukromí v prostředích B2C, v prostředích s rozsáhlou analytikou, s využitím adtech a s intenzivní správou souhlasů, aniž by zaváděla nekanonické registry, role nebo duplicitní pracovní postupy.

3. Cíle

3.1 Cílem této politiky je:

- 3.1.1 Zajistit, aby marketingové a sledovací účely byly zaznamenány před zahájením zpracování.
- 3.1.2 Zajistit, aby důkazy o souhlasu, preferencích, supresi a odvolání byly vedeny v kanonických důkazních objektech.
- 3.1.3 Zajistit, aby oznámení o cookies a marketingová oznámení byla aktuální, vedená v režimu správy verzí a propojená se záznamy o zpracování.
- 3.1.4 Zajistit, aby sledovací technologie, tagy, pixely, SDK, analytické nástroje a adtech integrace byly schváleny před použitím v produkčním prostředí.
- 3.1.5 Zajistit, aby marketingoví dodavatelé, poskytovatelé analytiky a reklamní partneři byli klasifikováni a řízení prostřednictvím kanonických důkazů o vztazích.
- 3.1.6 Zajistit jednotné směřování odhlášení, námitek, odvolání a stížností týkajících se přímého marketingu.
- 3.1.7 Zajistit směřování mezinárodního předávání pro marketingové dodavatele a poskytovatele analytiky, kde se použije.
- 3.1.8 Zajistit, aby opatření pro kampaně a sledování byla monitorována, přezkoumávána a zlepšována s využitím důkazů PIMS.

4. Prohlášení politiky

4.1 Evidence marketingového a sledovacího zpracování

- 4.1.1 [Controller] Process Owner / Business Owner musí před zahájením kampaně nebo sledovací činnosti zaznamenat každou marketingovou kampaň, kanál, účel zpracování, kategorii PII, zdroj publika, vazbu na právní základ, kategorii sledovací technologie, závislost na dodavateli nebo tagu, vazbu na oznámení, závislost na souhlasu nebo preferenci, vazbu na uchovávání a příznak předávání v REG02.
- 4.1.2 [Controller] Privacy Lead / PIMS Manager musí před spuštěním kampaně potvrdit, že každý marketingový účel v REG02 má aktuální vazbu na oznámení v REG07 a vazbu na souhlas nebo preferenci v REG05.
- 4.1.3 [Processor] Process Owner / Business Owner musí před zpracováním marketingových PII jménem správce dokumentovat zákazníkem schválené marketingové účely a pokyny zákazníka v REG02 nebo REG08.
- 4.1.4 [Joint Controller] Privacy Lead / PIMS Manager musí před spuštěním společného marketingu, kampaně se sdíleným publikem, společně označené kampaně nebo sdílené sledovací činnosti zaznamenat rozdělení odpovědností společných správců v REG08.
- 4.1.5 [Conditional] Privacy Lead / PIMS Manager musí před spuštěním do produkčního prostředí směřovat marketingové činnosti zahrnující mezinárodního dodavatele, tag, poskytovatele analytiky, reklamní platformu, předání publika nebo předání v rámci sdílení údajů do REG09.
- 4.1.6 [Controller] Process Owner / Business Owner musí před aktivací zaznamenat požadavky na supresi, vyloučení nebo nekontaktování spojené s každým marketingovým účelem v REG05.

4.2 Opatření pro souhlas, preference a cookies

- 4.2.1 [Controller] Process Owner / Business Owner musí před shromažďováním nebo použitím v kampani určit, zda je pro každý marketingový kanál vyžadován souhlas, preference, námitka, smluvní pokyn nebo jiný schválený základ, a zaznamenat rozhodnutí v REG02 a REG05.
- 4.2.2 [Controller] System Owner / Application Owner musí před nasazením nakonfigurovat neesenciální cookies, tagy, pixely, SDK a podobné sledovací technologie tak, aby zůstaly neaktivní, dokud není v REG05 dostupný požadovaný stav souhlasu nebo preference.
- 4.2.3 [Controller] System Owner / Application Owner musí před vydáním ověřit, že signály souhlasu nebo preferencí nejsou přepsány, obcházeny ani ignorovány během změn webu, aplikace, kampaně nebo správce značek, a zaznamenat důkazy o ověření v REG05 nebo REG12.
- 4.2.4 [Controller] Process Owner / Business Owner musí do jednoho pracovního dne po zachycení, změně nebo odvolání zaznamenat důkazy o souhlasu, preferenci, odvolání, supresi a verzi v REG05.
- 4.2.5 [Processor] System Owner / Application Owner musí v zákazníkem dohodnuté lhůtě uplatnit zákazníkem poskytnuté údaje o souhlasu, preferenci, supresi nebo pokynech v marketingových nástrojích spravovaných zpracovatelem a zaznamenat dokončení v REG05 nebo REG08.
- 4.2.6 [Conditional] Privacy Lead / PIMS Manager musí před vydáváním potvrzení o souhlasu pro marketingové účely, cookies nebo sledovací účely udržovat mapování polí potvrzení o souhlasu v REG05.

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

9. Výjimky

- 9.1 [All] Process Owner / Business Owner musí před použitím jakéhokoli nestandardního marketingového kanálu, tagu, analytické konfigurace, mechanismu preferencí nebo dodavatele, u něhož nelze před spuštěním dokončit požadované důkazy, požádat o výjimku v REG12.
- 9.2 [Conditional] Data Protection Officer / Privacy Advisor musí před schválením přezkoumat žádost o výjimku z ochrany soukromí v marketingu v REG12, pokud výjimka ovlivňuje souhlas, děti, zaměstnance, citlivá publika, přeshraniční předávání, profilování nebo významné rozšíření sledování.
- 9.3 [All] Top Management musí před nabytím účinnosti výjimky schválit vysoce rizikové nebo významné výjimky z ochrany soukromí v marketingu v REG12.
- 9.4 [All] Privacy Lead / PIMS Manager musí před schválením u každé schválené výjimky z ochrany soukromí v marketingu nastavit datum ukončení platnosti, vlastníka nápravy a datum přezkumu v REG12.

10. Uplatňování politiky

- 10.1 [All] Privacy Lead / PIMS Manager musí pozastavit nebo zablokovat marketingovou činnost v REG12, pokud před spuštěním nebo pokračujícím použitím chybí požadované důkazy v REG02, REG05, REG07, REG08 nebo REG09.
- 10.2 [All] System Owner / Application Owner musí do jednoho pracovního dne po rozhodnutí o uplatnění politiky deaktivovat neschválené tagy, trackery, pixely, SDK nebo datové toky kampaně a zaznamenat dokončení v REG08 nebo REG12.
- 10.3 [All] Vendor / Procurement Owner musí zablokovat onboarding, obnovení nebo rozšíření marketingového dodavatele, poskytovatele analytiky nebo reklamní platformy, pokud před zahájením nebo pokračováním zpracování chybí požadované důkazy v REG08 nebo REG09.

- 10.4 [All] Process Owner / Business Owner musí do jednoho pracovního dne po potvrzeném selhání opatření pro preference, supresi, oznámení nebo dodavatele zastavit používání dotčených PII v kampani a zaznamenat dokončení v REG05 nebo REG12.
- 10.5 [All] Internal Audit / Compliance Reviewer musí do 60 dnů po uzavření nápravného opatření ověřit účinnost nápravného opatření pro závažné nebo opakované neshody v ochraně soukromí v marketingu v REG12.

11. Přezkum a údržba

- 11.1 [All] Privacy Lead / PIMS Manager musí tuto politiku přezkoumat v REG12 každoročně a do 30 dnů po významné změně požadavků na marketing, cookies, sledování, analytiku, adtech nebo správu souhlasů.
- 11.2 [Controller] Process Owner / Business Owner musí alespoň čtvrtletně a do 30 dnů po významné změně kampaně přezkoumat záznamy marketingového zpracování v REG02 a závislosti preferencí v REG05.
- 11.3 [Controller] Privacy Lead / PIMS Manager musí alespoň jednou ročně a do 30 dnů po významné změně oznámení, sledování nebo preferencí přezkoumat záznamy marketingového oznámení a oznámení o cookies v REG07.
- 11.4 [All] Vendor / Procurement Owner musí alespoň jednou ročně a před obnovením přezkoumat záznamy marketingových dodavatelů, tagů, analytiku a reklamních platform v REG08.
- 11.5 [Conditional] Privacy Lead / PIMS Manager musí do 15 pracovních dnů po zjištěné změně marketingového dodavatele, poskytovatele analytiku nebo umístění hostingu aktualizovat směřování předávání v REG09.
- 11.6 [All] Top Management musí před zveřejněním schválit významné revize této politiky v REG12.

12. Související politiky

- 12.1 Tato politika je podporována následujícími souvisejícími politikami:
- 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 souhlasu a správy preferencí
- 12.7 PII06 - Politika správy práv subjektů PII
- 12.8 PII07 - Politika posouzení rizik pro soukromí a DPIA
- 12.9 PII08 - Politika ochrany soukromí již od návrhu a ve výchozím nastavení
- 12.10 PII09 - Politika shromažďování, použití, zpřístupňování a sdílení PII
- 12.11 PII10 - Politika uchovávání, výmazu a likvidace PII
- 12.12 PII11 - Politika přesnosti a kvality PII
- 12.13 PII12 - Politika správy ochrany soukromí u zpracovatelů, dílčích zpracovatelů a třetích stran
- 12.14 PII13 - Politika mezinárodního předávání PII
- 12.15 PII14 - Politika bezpečnosti PII a řízení přístupu
- 12.16 PII15 - Politika řízení incidentů a porušení zabezpečení týkajících se PII
- 12.17 PII17 - Politika dokumentovaných informací a správy důkazů PIMS
- 12.18 PII18 - Politika monitorování, auditu a zlepšování PIMS

- 12.19 PII19 - Politika ochrany osobních údajů zaměstnanců
- 12.20 PII20 - Politika ochrany soukromí dětí
- 12.21 PII21 - Politika ochrany soukromí při AI a automatizovaném rozhodování
- 12.22 PII23 - Politika cloudového zpracovatele PII

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 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1; 7.2; 7.6; 11.1].
- 13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.3.6; 4.5.5; 4.6.5; 4.7.4; 6.1; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.5; 11.1].
- 13.4 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.4; Annex A.1.2.5; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.6; 4.2.1; 4.2.4; 4.2.6; 4.5.1; 4.7.2; 7.1; 11.2].
- 13.5 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 5.6; 6.4; 7.5; 11.4].
- 13.6 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4; Annex A.1.3.5. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 7.3; 11.3].
- 13.7 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.10. Addressed by clauses [4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 7.2].
- 13.8 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5. Addressed by clauses [4.1.1; 4.2.2; 4.4.4; 4.5.1; 4.5.2; 4.5.4; 4.5.5; 4.7.2; 7.2].
- 13.9 ISO/IEC 27701:2025 - Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5. Addressed by clauses [4.1.5; 4.4.3; 4.4.6; 7.5; 11.5].
- 13.10 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.3; 4.2.5; 4.3.4; 4.4.5; 7.4].
- 13.11 ISO/IEC 27701:2025 - Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.2.5; 4.3.4; 4.4.6; 4.6.3; 7.4; 7.5].
- 13.12 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.2.3; 4.4.4; 4.7.1; 4.7.3; 5.7; 7.2; 10.2].
- 13.13 GDPR - Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(2). Addressed by clauses [4.1.1; 4.1.2; 4.1.6; 4.5.1; 4.5.2; 4.7.2; 8.1].
- 13.14 GDPR - Article 6; Article 7. Addressed by clauses [4.2.1; 4.2.2; 4.2.4; 4.2.6; 4.6.2; 7.2].
- 13.15 GDPR - Article 12; Article 13; Article 14. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.5; 11.3].
- 13.16 GDPR - Article 21. Addressed by clauses [4.5.2; 4.6.1; 4.6.2; 4.6.4; 8.3].
- 13.17 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32. Addressed by clauses [4.1.3; 4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 4.7.3; 5.6; 5.7; 6.2; 6.4; 8.4; 10.3].
- 13.18 GDPR - Article 44. Addressed by clauses [4.1.5; 4.4.6; 7.5; 11.5].
- 13.19 ISO/IEC 29100:2020 - Clause 5.1; Clause 5.8; Clause 5.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.3; 4.6.1; 4.6.2].
- 13.20 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.5.1; 4.5.2; 4.5.4; 4.7.2].
- 13.21 ISO/IEC 29100:2020 - Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.3.6; 4.5.5; 4.6.5; 4.7.1; 4.7.3; 4.7.4; 6.1; 8.5; 10.5].

13.22 ISO/IEC 29151:2022 - Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10.
Addressed by clauses [4.2.1; 4.2.2; 4.2.4; 4.5.1; 4.5.2; 4.6.1; 4.6.2; 7.2].

13.23 ISO/IEC TS 27560:2023 - Clause 5.2; Clause 5.3; Clause 6.2; Clause 6.4. Addressed by
clauses [4.2.4; 4.2.6; 7.1; 7.2].