					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: PII08					Dokumenttitel: **Policy för integritetsskydd genom design och dataskydd som standard**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Ansluten till standarder och regelverk

Standard / regelverk	Klausul / kontroll / artikel	Tillämplighet	Täckningstyp	Kommentar
ISO/IEC 27701:2025	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Koppling mellan bedömning och riskbehandling av integritetsrisker
ISO/IEC 27701:2025	Clause 6.3; Clause 8.1	Both	Primary	Planerade ändringar och operativ styrning
ISO/IEC 27701:2025	Clause 7.5	Both	Supporting	Dokumenterat underlag för integritetsskydd genom design
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Övervakning och korrigerande åtgärder
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9	Controller	Supporting	Ändamål, PIA-utlösare och register
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3	Controller	Primary	Begränsa insamling och behandling
ISO/IEC 27701:2025	Annex A.1.4.4; Annex A.1.4.5	Controller	Supporting	Mål för korrekthet och minimering
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7	Controller	Supporting	Design för avidentifiering, radering och temporära filer
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Kundavtal, stöd och register för personuppgiftsbiträde
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Supporting	Designförmågor för personuppgiftsbiträde
ISO/IEC 27701:2025	Annex A.3.27; Annex A.3.29	Both	Supporting	Utvecklingslivscykel och konstruktionsprinciper
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Supporting	Ändamålsbegränsning, minimering och ansvarsskyldighet
GDPR	Article 24	Controller	Supporting	Åtgärder för personuppgiftsansvarig
GDPR	Article 25	Controller	Primary	Dataskydd genom design och som standard

GDPR	Article 28	Both	Supporting	Instruktioner och bistånd för personuppgiftsbiträde
GDPR	Article 30	Both	Supporting	Register över behandling
GDPR	Article 35	Controller	Supporting	Koppling till DPIA-utlösare
ISO/IEC 29100:2020	Clause 4.7	Both	Supporting	Dataskyddskontroller genom design
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Ändamål, insamling, minimering och begränsning av användning
ISO/IEC 29100:2020	Clause 5.7; Clause 5.10; Clause 5.12	Both	Supporting	Korrekthet, ansvarsskyldighet och efterlevnad
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8	Both	Primary	Principer och kontroller för skydd av PII

1. Omfattning

1.1 Denna policy fastställer krav för att integrera integritetsskydd genom design och dataskydd som standard i nya och ändrade behandlingsaktiviteter, projekt, produkter, tjänster, system, applikationer, integrationer, upphandlingsaktiviteter och ändringar av verksamhetsprocesser som involverar PII inom PIMS-omfattningen.

1.2 Denna policy gäller sammanhang som personuppgiftsansvarig, gemensamt personuppgiftsansvarig, personuppgiftsbiträde och underbiträde.

1.3 Skyldigheter för personuppgiftsbiträde och underbiträde gäller när organisationen utformar, konfigurerar, ändrar eller driver behandling för en kunds, personuppgiftsansvarigs eller överordnat personuppgiftsbiträdes räkning enligt dokumenterade instruktioner.

1.4 Denna policy omfattar:

1.4.1 integritetskrav vid projektinitiering;

1.4.2 designkontroller för ändamål, uppgiftsminimering och standardinställningar;

1.4.3 granskning av inbyggt dataskydd före produktionssättning;

1.4.4 ändringsutlöst granskning av inbyggt dataskydd;

1.4.5 kontroller av inbyggt dataskydd vid upphandling;

1.4.6 koppling till integritetsrisk, DPIA-screening och underlag för korrigerande åtgärder.

1.5 Denna policy ersätter inte:

1.5.1 PII03 för behandlingsregister, ändamål, rättslig grund och ROPA-poster;

1.5.2 PII04 för innehåll i integritetsmeddelande och publicering;

1.5.3 PII05 för kontroller av samtycke och preferenser;

1.5.4 PII06 för hantering av registrerades rättigheter;

1.5.5 PII07 för metodik för bedömning av integritetsrisker och DPIA;

1.5.6 PII09 för kontroller av insamling, användning, röjande och delning;

1.5.7 PII10 för genomförande av bevarande, radering och bortskaffning;

1.5.8 PII11 för drift av korrekthet och kvalitet;

1.5.9 PII12 för livscykelstyrning av personuppgiftsbiträden, underbiträden och tredje parter;

1.5.10 PII13 för mekanismer för internationella överföringar;

1.5.11 PII14 för drift av PII-säkerhet och åtkomstkontroll;

1.5.12 PII18 för PIMS-övergripande övervakning, revision, korrigerande åtgärder och förbättringsstyrning.

2. Syfte

2.1 Syftet med denna policy är att säkerställa att integritetskrav identifieras, genomförs och beläggs innan behandling av PII påbörjas eller ändras väsentligt, samt att system och processer som standard konfigureras för att begränsa insamling, användning, exponering, beroende av bevarande, beroende av röjande och identifierbarhet av PII till vad som är nödvändigt för det dokumenterade ändamålet.

3. Mål

3.1 Målen med denna policy är att:

3.1.1 integrera integritetskrav i beslut om projektinitiering, design, upphandling, ändringar och produktionssättning;

3.1.2 säkerställa att design för behandling av PII är kopplad till dokumenterade ändamål och behandlingsposter i REG02;

3.1.3 införa uppgiftsminimering och integritetsskyddande standardinställningar innan behandling påbörjas;

3.1.4 säkerställa att integritetsrisk och DPIA-screening utlöses utan att metodiken i PII07 dupliceras;

3.1.5 säkerställa att krav på upphandling och design för personuppgiftsbiträden dokumenteras utan att livscykelstyrningen i PII12 dupliceras;

3.1.6 säkerställa att olösta designfrågor eskaleras via REG12;

3.1.7 upprätthålla designunderlag med beredskap för revision i REG02, REG04, REG08 och REG12.

4. Policyuttalanden

4.1 Projektinitiering och integritetskrav

4.1.1 [Both] The Process Owner / Business Owner MUST registrera en post om inbyggt dataskydd i REG04 innan något projekt, någon produkt, tjänst, system, applikation, integration eller ändring av verksamhetsprocess som involverar PII initieras.

4.1.2 [Both] The Process Owner / Business Owner MUST koppla varje post om inbyggt dataskydd i REG04 till en befintlig eller preliminär behandlingsaktivitet i REG02 innan funktionella krav godkänns.

4.1.3 [Controller] The Privacy Lead / PIMS Manager MUST dokumentera krav på integritetsskydd genom design för personuppgiftsansvarig i REG04 innan funktionell design för personuppgiftsansvarig godkänns.

4.1.4 [Processor] The Vendor / Procurement Owner MUST dokumentera kundinstruktioner om integritetsdesign och avtalsmässiga designbegränsningar i REG08 innan tjänstedesign eller väsentlig tjänsteförändring för personuppgiftsbiträde godkänns.

4.1.5 [Conditional] The Data Protection Officer / Privacy Advisor MUST dokumentera rådgivning i REG04 innan en PII-design som är högrisk, ny, känslig, automatiserad, storskalig eller väsentligt ändrad godkänns.

4.1.6 [Both] The Information Security Lead MUST dokumentera beroenden till säkerhetskontroller för PII som stödjer integritetsdesignen i REG04 innan arkitekturen godkänns.

4.2 Uppgiftsminimering och design för dataskydd som standard

4.2.1 [Controller] The Process Owner / Business Owner MUST dokumentera minsta nödvändiga PII-kategorier, kategorier av registrerade, källor och ändamål i REG02 och REG04 innan design för insamling eller import godkänns.

4.2.2 [Both] The System Owner / Application Owner MUST konfigurera standardinställningar för behandling till den minsta insamling och behandling av PII som behövs för det dokumenterade ändamålet och dokumentera underlag i REG04 innan systemet tas i produktion.

4.2.3 [Controller] The Process Owner / Business Owner MUST dokumentera frivilliga PII-fält, frivilliga behandlingsval och standardinställningar som är avstängda som standard i REG02 och REG04 innan användargränssnitt, formulär eller arbetsflöde godkänns.

4.2.4 [Both] The System Owner / Application Owner MUST dokumentera dataskyddsvänliga standardinställningar för exponering i vyer, rapporter, exporter, gränssnitt och automatiserade arbetsflöden i REG04 innan systemet tas i produktion.

4.2.5 [Both] The Process Owner / Business Owner MUST dokumentera genomförbarheten av avidentifiering, pseudonymisering, aggregering eller icke-identifierbar behandling i REG04 innan identifierbar PII godkänns för testning, analys, rapportering eller sekundär operativ användning.

4.2.6 [Both] The System Owner / Application Owner MUST dokumentera hantering av tillfälliga PII-artefakter, inklusive temporära filer, cacheminnen, loggar eller stagingposter, i REG04 innan systemet tas i produktion.

4.2.7 [Both] The Process Owner / Business Owner MUST dirigera designkrav som ägs av PII10, PII11, PII13 eller PII14 till den relaterade policyns underlagssökväg i REG04 inom fem arbetsdagar från det att beroendet identifierades.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Undantag

9.1 Undantag för integritetsdesign

9.1.1 [Both] The Process Owner / Business Owner MUST begära ett undantag för integritetsdesign i REG12 innan en design eller ändring godkänns som inte kan uppfylla ett tillämpligt krav på integritetsdesign.

9.1.2 [Both] The Privacy Lead / PIMS Manager MUST bedöma påverkan, kompenserande kontroller och utgångsdatum för varje undantag för integritetsdesign i REG12 inom fem arbetsdagar från begäran.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST dokumentera rådgivning i REG12 innan ett undantag för integritetsdesign som involverar högriskbehandling, känslig, automatiserad, storskalig, omtvistad eller rättsligt väsentlig behandling godkänns.

9.1.4 [All] Top Management MUST godkänna ett undantag för integritetsdesign som påverkar behandling med hög påverkan, certifieringsomfattning, olöst större risk eller rättslig skyldighet i REG12 innan undantaget får verkan.

9.1.5 [Both] The Privacy Lead / PIMS Manager MUST ange ett utgångsdatum som inte överstiger 90 dagar i REG12 för varje godkänt undantag för integritetsdesign före godkännande.

9.1.6 [Both] The Privacy Lead / PIMS Manager MUST stänga eller ompröva varje undantag för integritetsdesign i REG12 inom fem arbetsdagar från utgångsdatum.

10. Tillämpning

10.1 Tillämpning och hantering av avvikelser

10.1.1 [Both] The Privacy Lead / PIMS Manager MUST registrera saknad granskning av inbyggt dataskydd, saknat underlag för minimering, olöst fel i standardinställningar eller otillåten produktionssättning som en avvikelse i REG12 inom fem arbetsdagar efter identifiering.

10.1.2 [Both] The System Owner / Application Owner MUST förhindra produktionssättning av ett system som behandlar PII när granskningen av inbyggt dataskydd i REG04 är ofullständig och dokumentera beslutet i REG12 före produktionssättning.

10.1.3 [Both] The Vendor / Procurement Owner MUST förhindra leverantörsintroduktion eller avtalssignering när erforderligt underlag för integritetsdesign i REG08 saknas och dokumentera beslutet i REG12 före introduktion eller signering.

10.1.4 [Both] The Process Owner / Business Owner MUST pausa användningen av ny eller ändrad design för behandling av PII tills REG04-granskning, REG02-uppdateringar och erforderliga REG12-undantag är slutförda.

10.1.5 [All] Top Management MUST kräva korrigerande åtgärder i REG12 inom 10 arbetsdagar vid upprepade, långvariga eller högpåverkande brister i integritetsdesign.

10.1.6 [All] The Internal Audit / Compliance Reviewer MUST verifiera effektiviteten hos korrigerande åtgärder för avvikelser i integritetsdesign i REG12 vid nästa planerade PIMS-revision eller inom 60 dagar efter stängning, beroende på vilket som inträffar först.

11. Granskning och underhåll

11.1 Granskning av policy och designkontroller

11.1.1 [All] The Privacy Lead / PIMS Manager MUST granska denna policy i REG12 årligen och inom 30 dagar efter väsentlig ändring av rättsliga krav, behandling, teknik, certifieringsomfattning eller PIMS-kontroll.

11.1.2 [Both] The Process Owner / Business Owner MUST granska aktiva behandlingsaktiviteter i REG02 avseende ändringar i beroenden till integritetsdesign årligen och inom 30 dagar efter väsentlig ändring av behandling.

11.1.3 [Both] The System Owner / Application Owner MUST granska underlag för dataskyddsvänlig standardkonfiguration i REG04 årligen och inom 30 dagar efter väsentlig systemändring.

11.1.4 [Both] The Vendor / Procurement Owner MUST granska skyldigheter för integritetsdesign avseende leverantörer, personuppgiftsbiträden, underbiträden och tredje parter i REG08 före förnyelse och inom 30 dagar efter väsentlig ändring av relationen.

11.1.5 [Conditional] The Data Protection Officer / Privacy Advisor MUST granska integritetspåverkan av väsentliga policyändringar i REG12 före godkännande.

11.1.6 [All] Top Management MUST godkänna väsentliga ändringar av denna policy i REG12 före publicering.

12. Relaterade policyer

12.1 PII01 - Policy för ledningssystem för hantering av integritetsinformation

12.2 PII02 - Policy för integritetsroller, ansvar och ansvarsskyldighet

12.3 PII03 - Policy för behandlingsregister för PII och rättslig grund

12.4 PII04 - Policy för integritetsmeddelande och transparens

12.5 PII05 - Policy för hantering av samtycke och preferenser

12.6 PII06 - Policy för hantering av registrerades rättigheter

12.7 PII07 - Policy för bedömning av integritetsrisker och DPIA

12.8 PII09 - Policy för insamling, användning, röjande och delning av PII

12.9 PII10 - Policy för bevarande, radering och bortskaffning av PII

12.10 PII11 - Policy för korrekthet och kvalitet avseende PII

12.11 PII12 - Policy för integritetshantering av personuppgiftsbiträden, underbiträden och tredje parter

12.12 PII13 - Policy för internationella PII-överföringar

12.13 PII14 - Policy för PII-säkerhet och åtkomstkontroll

12.14 PII17 - Policy för dokumenterad information och bevismaterial i PIMS

12.15 PII18 - Policy för övervakning, revision och förbättring i PIMS

13. Referensstandarder och ramverk

13.1 Denna policy är mappad mot följande standarder och regelverk. Mappningen förklarar hur policyn stödjer de angivna kraven och identifierar de interna klausuler som genomför eller stödjer dem.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.2; Clause 6.1.3** - Mappad mot screening av integritetsrisker, koppling till behandlingsåtgärder, analys av designberoenden, eskalering och korrigerande åtgärder utan att den fullständiga metodiken för integritetsrisk och DPIA dupliceras. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.5; 5.1.3; 7.1.7].

13.2.2 **Clause 6.3; Clause 8.1** - Mappad mot planerade integritetsändringar, projektinitiering, operativ granskning av inbyggt dataskydd, kontroll inför produktionssättning och granskning av

väsentliga ändringar. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.3; 4.3.5; 4.5.1; 4.5.3; 4.5.4; 4.5.6; 7.1.2; 7.1.5; 10.1.2].

13.2.3 **Clause 7.5** - Mappad mot dokumenterat underlag för integritetsdesign som bevaras i REG02, REG04, REG08 och REG12. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 5.1.2; 5.1.5; 5.1.6; 5.1.7; 7.1.1; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1; Clause 10.2** - Mappad mot mätetal för integritetsdesign, stickprov på underlag, registrering av avvikelser, korrigerande åtgärder och verifiering av effektivitet. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 6.1.1; 6.1.2; 6.1.4; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.5; 10.1.6].

13.2.5 **Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9** - Mappad mot dokumentation av behandlingsändamål, behandlingsregister, koppling till integritetsdesign och utlösare för integritetsrisk eller DPIA-screening vid behandling där organisationen är personuppgiftsansvarig. Addressed by clauses [4.1.2; 4.2.1; 4.3.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3** - Mappad mot begränsning av insamling och behandling av PII genom ändamålsbaserade minimikrav på data, frivillig behandling som är avstängd som standard och minsta standardinställningar för behandling. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.5.4; 7.1.5; 11.1.3].

13.2.7 **Annex A.1.4.4; Annex A.1.4.5** - Mappad mot dirigering av korrekthetsberoenden, minimeringsmål, genomförbarhet av avidentifiering och designunderlag för att minimera identifierbar PII. Addressed by clauses [4.2.5; 4.2.7; 4.3.2; 4.5.2; 7.1.3; 11.1.2].

13.2.8 **Annex A.1.4.6; Annex A.1.4.7** - Mappad mot identifiering i designfasen av avidentifiering, beroende av radering, temporära PII-artefakter och dirigering till livscykelkontroller utan att genomförande av bevarande eller bortskaffning dupliceras. Addressed by clauses [4.2.5; 4.2.6; 4.2.7; 4.3.3; 4.5.4; 7.1.5; 11.1.3].

13.2.9 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Mappad mot kundinstruktioner till personuppgiftsbiträde, kundstödsinformation, designregister för personuppgiftsbiträde och kundgodkända ändringar av tjänstedesign. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.6; 5.1.7; 7.1.4; 11.1.4].

13.2.10 **Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4** - Mappad mot designförmågor hos personuppgiftsbiträde avseende temporära filer, beroende av återlämnande eller bortskaffning och beroende av överföringskontroll, dokumenterade som designunderlag utan att operativa rutiner för radering eller säkerhetskontroller dupliceras. Addressed by clauses [4.2.6; 4.2.7; 4.4.3; 4.4.4; 4.4.6; 7.1.4; 7.1.6; 11.1.4].

13.2.11 **Annex A.3.27; Annex A.3.29** - Mappad mot integritetskrav i utvecklingslivscykel, konstruktionsprinciper, kontrollpunkter för skydd av PII och underlag för dataskyddsvänlig standardkonfiguration. Addressed by clauses [4.1.6; 4.3.3; 4.3.4; 4.4.4; 4.5.1; 4.5.4; 5.1.4; 5.1.6; 7.1.5; 7.1.6; 10.1.2; 11.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Mappad mot ändamålsbegränsning, minsta PII-design, koppling till behandlingsregister, minimering som standard, underlag och ansvarsskyldighet. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.2; 4.5.2; 5.1.5; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Mappad mot åtgärder för personuppgiftsansvarig, styrningsgranskning, godkännande av undantag, korrigerande åtgärder och policyunderhåll för genomförande av integritetsskydd genom design. Addressed by clauses [4.1.3; 4.5.6; 5.1.1; 6.1.2; 9.1.2; 9.1.4; 10.1.5; 11.1.6].

13.3.3 **Article 25** - Mappad mot projektinitiering, integritetskrav i designfasen, dataskyddsvänliga standardinställningar, minimering, upphandlingskontroller av design, granskning inför produktionssättning och ändringsutlöst granskning. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.5; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 10.1.2].

13.3.4 **Article 28** - Mappad mot instruktioner till personuppgiftsbiträde, designstöd från personuppgiftsbiträde, underlag för leverantörers integritetsdesign och kundgodkända designändringar. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.5; 4.4.6; 5.1.7; 7.1.4; 10.1.3; 11.1.4].

13.3.5 **Article 30** - Mappad mot koppling till behandlingsregister, uppdateringar av REG02, designberoenden för behandlingsaktiviteter och underlag för behandlingsregister. Addressed by clauses [4.1.2; 4.2.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.3.6 **Article 35** - Mappad mot utlösare för integritetsrisk och DPIA-screening i designfasen, rådgivning vid hög risk och kontroller efter införande utan att DPIA-metodiken dupliceras. Addressed by clauses [4.1.5; 4.3.1; 4.3.6; 5.1.3; 6.1.3; 9.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7** - Mappad mot identifiering av dataskyddskontroller i designfasen, koppling till integritetsrisk och designunderlag för genomförande av kontroller. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.5.1].

13.4.2 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mappad mot ändamålsspecificering, insamlingsbegränsning, uppgiftsminimering, begränsad användning och standardinställningar för behandling. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.4.2; 4.5.2].

13.4.3 **Clause 5.7; Clause 5.10; Clause 5.12** - Mappad mot dirigering av korrekthetsberoenden, underlag för ansvarsskyldighet, övervakning av integritetsdesign, revision och korrigerande åtgärder. Addressed by clauses [4.2.7; 4.3.6; 4.5.5; 6.1.1; 6.1.4; 8.1.1; 8.1.2; 10.1.1; 10.1.6].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8** - Mappad mot ändamålets legitimitet, insamlingsbegränsning, uppgiftsminimering, begränsning av användning och röjande, beroende av bevarande, hantering av temporära filer och designkontroller för korrekthetsberoenden. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.4.2; 4.5.2; 4.5.4; 7.1.3; 7.1.5].