

				Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: PII04				Dokumenttitel: Policy för integritetsmeddelanden och transparens							
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

<p>Juridiskt meddelande (upphovsrätt och användningsbegränsningar) (C) 2025 Clarysec LLC. All rights reserved.</p> <p>Detta dokument är Clarysec LLC:s immateriella egendom. Ingen del av detta dokument får kopieras, återanvändas, distribueras eller ändras för kommersiella eller implementeringsändamål utan uttryckligt skriftligt förhandstillstånd.</p> <p>Obehörig användning är strängt förbjuden och kan leda till rättsliga åtgärder.</p> <p>För licensiering, kontakta: info@clarysec.com</p>

Ansluten till standarder och regelverk

Standard / regelverk	Klausul / kontroll / artikel	Tillämplighet	Täckningstyp	Kommentar
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Dokumenterad information om meddelanden och operativ styrning
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Övervakning av meddelanden och korrigerande åtgärder
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.9	Controller	Supporting	Koppling mellan ändamål, rättslig grund och register över behandling
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4	Controller	Primary	Informations- och transparenskyldigheter gentemot registrerade
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Transparensinformation för gemensamt personuppgiftsansvarig
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.3.2	Processor	Supporting	Stöd från personuppgiftsbiträde för personuppgiftsansvarigs skyldigheter avseende meddelanden
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Transparens och ansvarsskyldighet
GDPR	Article 12	Controller	Primary	Transparent information och kommunikation
GDPR	Article 13	Controller	Primary	Information när PII samlas in från den registrerade
GDPR	Article 14	Controller	Primary	Information när PII inte erhålls från den registrerade
GDPR	Article 24	Controller	Supporting	Styrningsåtgärder för personuppgiftsansvarig
GDPR	Article 26	Joint Controller	Supporting	Transparens vid gemensamt personuppgiftsansvar
GDPR	Article 28	Processor	Supporting	Stöd för personuppgiftsbitrådets assistans och instruktioner

GDPR	Article 30	Both	Supporting	Koppling till register över behandling
ISO/IEC 29100:2020	Clause 5.3; Clause 5.8; Clause 5.10	Both	Supporting	Principer om ändamål, transparens och ansvarsskyldighet
ISO/IEC 29151:2022	Annex A.9.1; Annex A.9.2	Controller	Supporting	Kontroller för integritetsmeddelanden, öppenhet och transparens
ISO/IEC 29184:2020	Clause 5.1; Clause 5.2; Clause 5.3	Controller	Supporting	Syfte, tillhandahållande och innehåll för meddelanden online

1. Omfattning

1.1 Denna policy anger krav för att skapa, godkänna, publicera, underhålla, granska och belägga integritetsmeddelanden och transparensinformation för behandling av PII inom PIMS-omfattningen.

1.2 Denna policy gäller för:

1.2.1 integritetsmeddelanden för behandlingsaktiviteter där organisationen är personuppgiftsansvarig;

1.2.2 transparensinformation för behandlingsaktiviteter vid gemensamt personuppgiftsansvar;

1.2.3 stöd från personuppgiftsbiträden och underbiträden för personuppgiftsansvarigs skyldigheter avseende meddelanden när organisationen agerar enligt dokumenterade kund- eller biträdesinstruktioner;

1.2.4 koppling av meddelandehåll till behandlingsändamål i REG02, referenser till rättslig grund, PII-kategorier, kategorier av registrerade, källkategorier, mottagarkategorier, bevarandereferenser och överföringsreferenser;

1.2.5 publicering av meddelanden via digitala, fysiska, avtalsmässiga, tjänste-, produkt-, formulär-, skyltnings-, skiktade, kortforms- och just-in-time-kanaler;

1.2.6 uppgifter om språk, version, godkännande, publicering och granskning av meddelanden som underhålls i REG07;

1.2.7 hänvisningar till kanaler för rättighetsbegäranden och integritetskontakt som är kopplade till REG06;

1.2.8 övervakning, undantag, avvikelser, korrigerande åtgärder och förbättringsunderlag som underhålls i REG12.

1.3 Denna policy anger inte krav för inhämtning av samtycke, genomförande av återkallelse av samtycke, preferenshantering, mottagning av rättighetsbegäranden, verifiering av rättighetsbegäranden, uppfyllande av rättighetsbegäranden, metodik för DPIA, genomförande av bevarande, val av mekanism för internationell överföring, kommunikation vid personuppgiftsincident eller förhandling av avtal med personuppgiftsbiträde. Dessa krav anges i de relaterade policyer som förtecknas i avsnitt 12.

1.4 I denna policy avser integritetsmeddelande godkänd extern information som tillhandahålls registrerade eller berörda målgrupper och beskriver hur PII behandlas.

1.5 I denna policy avser integritetsväsentligt meddelande ett meddelande som omfattar högriskbehandling, särskilda kategorier av PII, uppgifter om fällande domar eller brott, behandling som rör barn, arbetstagar- eller övervakningssammanhang, automatiserat beslutsfattande eller profilering, indirekt insamling i stor skala, internationell överföring, behandling vid gemensamt personuppgiftsansvar eller något meddelande som är föremål för väsentlig rättslig, regulatorisk, avtalsmässig eller kundrelaterad granskning.

1.6 I denna policy avser väsentlig ändring av meddelande varje ändring av personuppgiftsansvarigs identitet, kontaktpunkt, behandlingsändamål, referens till rättslig grund, PII-kategori, kategori av registrerade, källkategori, mottagarkategori, bevarandereferens, överföringsreferens, kanal för rättighetsbegäranden, kanal för klagomål eller integritetskontakt, språktäckning, publiceringskanal eller behandlingskontext som påverkar den information som lämnas till registrerade.

2. Syfte

2.1 Syftet med denna policy är att säkerställa att registrerade får tydliga, aktuella, tillgängliga och revisionsbara integritetsmeddelanden före eller vid den tidpunkt som krävs i livscykeln för behandling av PII.

2.2 Denna policy säkerställer att innehållet i integritetsmeddelanden styrs genom REG07, anpassas till behandlingsregister i REG02, stöds av kontakt- och rättighetskanalreferenser i REG06 och granskas när behandling eller transparenskyldigheter ändras.

3. Mål

3.1 Målen med denna policy är att:

- 3.1.1 fastställa REG07 som det auktoritativa evidensobjektet för register över integritetsmeddelanden, godkännande, publicering, granskning, språk och uppgifter om versionshantering;
- 3.1.2 säkerställa att varje integritetsmeddelande för personuppgiftsansvarig kopplas till aktuella behandlingsändamål i REG02 före publicering;
- 3.1.3 säkerställa att integritetsmeddelanden innehåller godkänd transparensinformation som är anpassad till målgruppen och användbar externt;
- 3.1.4 ange tydliga godkännandansvar för innehåll i meddelanden före publicering eller aktivering av insamlingskanal;
- 3.1.5 säkerställa att meddelanden publiceras via relevanta digitala och icke-digitala kanaler innan PII samlas in eller används;
- 3.1.6 underhålla styrda meddelandeverisioner, översatta versioner, publiceringsunderlag och underlag för ersatta meddelanden i REG07;
- 3.1.7 säkerställa att uppdateringar av meddelanden utlöses av väsentliga ändringar i behandlingsregister i REG02 eller transparenskyldigheter;
- 3.1.8 tillhandahålla stöd från personuppgiftsbiträden och underbiträden för personuppgiftsansvarigs skyldigheter avseende meddelanden utan att duplicera styrningskontroller för personuppgiftsbiträden som ägs av PII12;
- 3.1.9 koppla integritetsmeddelandens kontakt- och rättighetsbegäransreferenser till REG06 utan att duplicera kontroller för rättighetshantering som ägs av PII06;
- 3.1.10 undvika att skapa separata formulär för godkännande av meddelanden eller register över meddelanden utanför REG07.

4. Policyuttalanden

4.1 Register över meddelanden och koppling till behandlingsändamål

- 4.1.1 [Controller] Process Owner / Business Owner MUST skapa en REG07-post för integritetsmeddelande som är kopplad till relevant behandlingsaktivitet i REG02 innan någon ny kanal, tjänst, blankett, kampanj, produkt eller funktion för insamling av PII i egenskap av personuppgiftsansvarig lanseras.
- 4.1.2 [Controller] Process Owner / Business Owner MUST skapa en REG07-post för integritetsmeddelande som är kopplad till relevant behandlingsaktivitet i REG02 innan PII som erhållits från annan källa än den registrerade används, före den första kommunikationen med den registrerade, före det första utlämnandet till tredje part eller inom 20 arbetsdagar efter att PII har erhållits, beroende på vilket som inträffar först.
- 4.1.3 [Controller] Privacy Lead / PIMS Manager MUST underhålla den godkända uppsättningen fält för meddelanden i REG07, inklusive meddelande-ID, ägare, kopplade REG02-poster, kanal, målgrupp, språk, version, ikraftträdandedatum, godkännandestatus och publiceringsplats, före inledande PIMS-drift och därefter årligen.
- 4.1.4 [Controller] Process Owner / Business Owner MUST koppla varje aktivt REG07-meddelande till varje aktuellt behandlingsändamål i REG02 som omfattas av meddelandet före godkännande av meddelandet och när REG02 ändras väsentligt.

- 4.1.5 [Joint Controller] Privacy Lead / PIMS Manager MUST registrera den publika sammanfattningen av ansvar vid gemensamt personuppgiftsansvar och kontaktpunkten i REG07 innan behandling vid gemensamt personuppgiftsansvar lanseras eller ändras väsentligt.
- 4.1.6 [Processor] Privacy Lead / PIMS Manager MUST registrera kundens information för stöd till meddelanden i REG07 och koppla den till REG02 inom 10 arbetsdagar efter mottagande av en godkänd kundinstruktion om att stödja ett meddelande från personuppgiftsansvarig.
- 4.1.7 [Subprocessor] Privacy Lead / PIMS Manager MUST registrera information för stöd till meddelanden som begärs av det instruerande personuppgiftsbiträdet i REG07 och koppla den till REG02 inom 10 arbetsdagar efter mottagande av en godkänd instruktion från personuppgiftsbiträdet.

4.2 Innehåll i meddelanden och transparensinformation

- 4.2.1 [Controller] Process Owner / Business Owner MUST inkludera personuppgiftsansvarigs identitet och aktuell integritetskontaktpunkt i REG07 innan ett integritetsmeddelande lämnas in för godkännande.
- 4.2.2 [Controller] Process Owner / Business Owner MUST inkludera varje kopplat behandlingsändamål i REG02 och referens till rättslig grund i REG07 innan ett integritetsmeddelande lämnas in för godkännande.
- 4.2.3 [Controller] Process Owner / Business Owner MUST inkludera PII-kategorier, kategorier av registrerade, källkategori när insamlingen är indirekt, mottagarkategorier, bevarandereferens och överföringsreferens från REG02 i REG07 innan ett integritetsmeddelande lämnas in för godkännande.
- 4.2.4 [Controller] Process Owner / Business Owner MUST inkludera aktuell mottagningskanal för rättighetsbegäranden enligt REG06 och kanal för klagomål eller integritetskontakt i REG07 innan ett integritetsmeddelande lämnas in för godkännande.
- 4.2.5 [Controller] Data Protection Officer / Privacy Advisor MUST registrera rådgivning i REG07 eller REG12 innan ett integritetsväsentligt meddelande godkänns.
- 4.2.6 [Controller] Privacy Lead / PIMS Manager MUST verifiera att meddelandehålllet i REG07 överensstämmer med REG02 innan meddelandet godkänns för publicering.
- 4.2.7 [Controller] Process Owner / Business Owner MUST registrera eventuell sammanfattning för skittat meddelande, kortformsmeddelande, skyltningstext eller just-in-time-meddelandetext i REG07 före publicering i relevant kanal.

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

9. Undantag

9.1 Undantagshantering

- 9.1.1 [All] Process Owner / Business Owner MUST registrera en begäran om undantag för meddelande i REG12 innan avvikelser från ett krav i denna policy sker.
- 9.1.2 [Controller] Data Protection Officer / Privacy Advisor MUST registrera rådgivning i REG12 innan något undantag som påverkar meddelandehåll, tidpunkt för indirekt insamling, integritetsväsentlig behandling eller REG06-kontaktreferenser godkänns.
- 9.1.3 [All] Top Management MUST godkänna varje undantag för meddelande som påverkar lansering av insamling, publiceringstidpunkt, högriskbehandling, transparens vid gemensamt personuppgiftsansvar eller kundåtagande för personuppgiftsbiträde i REG12 innan undantaget träder i kraft.

- 9.1.4 [All] Privacy Lead / PIMS Manager MUST registrera kompenserande transparensåtgärder, ägare, förfallodag och utgångsdatum i REG12 innan ett undantag för meddelande godkänns.
- 9.1.5 [All] Process Owner / Business Owner MUST stänga eller förnya ett godkänt undantag för meddelande i REG12 inom fem arbetsdagar före undantagets utgångsdatum.

10. Tillämpning

10.1 Avvikelse och korrigerande åtgärd

- 10.1.1 [All] Privacy Lead / PIMS Manager MUST registrera saknat, felaktigt, opublicerat, icke godkänt eller inaktuellt meddelandeunderlag som en avvikelse i REG12 inom fem arbetsdagar från identifiering.
- 10.1.2 [Controller] System Owner / Application Owner MUST blockera eller pausa driftsättning av insamlingskanal i REG12 när godkänt REG07-underlag för publicering av meddelande saknas före driftsättning.
- 10.1.3 [Controller] Privacy Lead / PIMS Manager MUST eskalera ett väsentligt felaktigt eller vilseledande meddelande till Data Protection Officer / Privacy Advisor och Top Management i REG12 inom två arbetsdagar från bekräftelse.
- 10.1.4 [Controller] Process Owner / Business Owner MUST registrera en plan för korrigerande åtgärder i REG12 inom 10 arbetsdagar efter tilldelning av en meddelanderelaterad avvikelse.
- 10.1.5 [All] Internal Audit / Compliance Reviewer MUST verifiera stängningsunderlag för meddelanderelaterade korrigerande åtgärder i REG12 vid nästa planerade revision eller inom 60 dagar från stängning, beroende på vilket som inträffar först.

11. Granskning och underhåll

11.1 Policygranskning och underhåll

- 11.1.1 [All] Privacy Lead / PIMS Manager MUST granska denna policy i REG12 årligen och inom 30 dagar efter en väsentlig ändring av meddelanden, transparens, rättsliga krav, regulatoriska krav, avtalskrav, behandling eller certifiering.
- 11.1.2 [All] Data Protection Officer / Privacy Advisor MUST granska integritetsväsentliga ändringar av denna policy i REG12 före godkännande.
- 11.1.3 [All] Top Management MUST godkänna väsentliga ändringar av denna policy i REG12 före publicering.
- 11.1.4 [All] Privacy Lead / PIMS Manager MUST uppdatera uppsättningen fält för meddelanden i REG07 inom 15 arbetsdagar efter godkända policyändringar som ändrar krav på meddelandeunderlag, godkännande, publicering, granskning, språk eller versionshantering.
- 11.1.5 [All] Privacy Lead / PIMS Manager MUST registrera kommunikation av godkända ändringar av denna policy i REG11 inom 30 dagar efter publicering.

12. Relaterade policyer

- 12.1 Denna policy stöds av följande relaterade policyer:
- 12.2 PII01 - Policy för ledningssystem för hantering av integritetsinformation
- 12.3 PII02 - Policy för integritetsroller, ansvar och ansvarsskyldighet
- 12.4 PII03 - Policy för inventering av PII-behandling och rättslig grund
- 12.5 PII05 - Policy för samtyckes- och preferenshantering
- 12.6 PII06 - Policy för hantering av registrerades rättigheter
- 12.7 PII07 - Policy för bedömning av integritetsrisker och DPIA
- 12.8 PII08 - Policy för integritetsskydd genom design och som standard
- 12.9 PII09 - Policy för insamling, användning, utlämnande och delning av PII
- 12.10 PII10 - Policy för bevarande, radering och bortskaffning av PII

- 12.11 PII11 - Policy för korrekthet och kvalitet i PII
- 12.12 PII12 - Policy för hantering av integritet hos personuppgiftsbiträden, underbiträden och tredje parter
- 12.13 PII13 - Policy för internationell överföring av PII
- 12.14 PII15 - Policy för incident- och personuppgiftsincidenthantering avseende PII
- 12.15 PII17 - Policy för dokumenterad information och evidenshantering i PIMS
- 12.16 PII18 - Policy för PIMS-övervakning, revision och förbättring

13. Referensstandarder och ramverk

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

13.2 ISO/IEC 27701:2025

- 13.2.1 **Clause 7.5; Clause 8.1** - Mappas till underhåll av dokumenterad information om integritetsmeddelanden, godkännandeunderlag, publiceringsunderlag, versionsuppgifter, poster om stöd från personuppgiftsbiträden och operativa kontroller före insamling eller publicering. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.5; 4.4.6; 4.6.1; 4.6.2; 4.6.4].
- 13.2.2 **Clause 9.1; Clause 10.2** - Mappas till övervakning av meddelanden, avstämning mellan REG07 och REG02, uppföljning av avvikelser, korrigerande åtgärder för meddelanden, undantag, tillämpning och effektivitetsgranskning. Addressed by clauses [4.5.3; 4.5.4; 4.5.5; 4.5.6; 6.1.2; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 10.1.1; 10.1.4; 10.1.5].
- 13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.9** - Mappas till koppling av ändamål och rättslig grund i REG02, poster om meddelanden för personuppgiftsansvarig behandling och register som stödjer meddelandeunderlag. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.2; 4.2.3; 4.2.6; 4.5.1; 4.5.2; 4.5.4].
- 13.2.4 **Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4** - Mappas till fastställande av skyldigheter avseende meddelanden, fastställande av information och tidpunkt för meddelanden samt tillhandahållande av tydlig och tillgänglig information från personuppgiftsansvarig till registrerade. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.5.1; 4.5.2; 4.5.3].
- 13.2.5 **Annex A.1.2.8** - Mappas till registrering av publik ansvarsfördelning och kontaktinformation vid gemensamt personuppgiftsansvar för transparens i meddelanden. Addressed by clauses [4.1.5; 4.2.1; 4.2.4].
- 13.2.6 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.3.2** - Mappas till stöd från personuppgiftsbiträden och underbiträden för personuppgiftsansvarigs skyldigheter avseende meddelanden genom kundinformation för stöd till meddelanden, beskrivningar av tjänstebehandling, tekniskt publiceringsstöd och eskalering av motstridiga begäranden om stöd till meddelanden. Addressed by clauses [4.1.6; 4.1.7; 4.6.1; 4.6.2; 4.6.3; 4.6.4].

13.3 GDPR

- 13.3.1 **Article 5(1)(a); Article 5(2)** - Mappas till transparens, evidensbaserat godkännande av meddelanden, REG07-publiceringsunderlag, bevarade meddelandeverioner, avstämning, korrigerande åtgärder och mätetal för ansvarsskyldighet. Addressed by clauses [4.1.3; 4.2.6; 4.3.5; 4.4.6; 4.5.4; 4.5.5; 4.5.6; 6.1.2; 8.1.1; 10.1.1].
- 13.3.2 **Article 12** - Mappas till tydlig, tillgänglig, målgruppsanpassad och språkstyrd meddelandeinformation samt publicering via tillämpliga digitala och icke-digitala kanaler. Addressed by clauses [4.2.4; 4.2.5; 4.2.7; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4].

- 13.3.3 **Article 13** - Mappas till information som tillhandahålls när PII samlas in från den registrerade, inklusive personuppgiftsansvarigs identitet, ändamål, referenser till rättslig grund, kategorier, mottagare, bevarande, överföringsreferenser och referenser till rättighetskanaler. Addressed by clauses [4.1.1; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4].
- 13.3.4 **Article 14** - Mappas till information som tillhandahålls när PII erhålls från annan källa än den registrerade, inklusive tidpunkt, källkategori, ändamål, kategorier, mottagare, bevarande, överföringsreferenser och referenser till rättighetskanaler. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.5.2].
- 13.3.5 **Article 24** - Mappas till styrningsåtgärder för personuppgiftsansvarig avseende fältuppsättningar för meddelanden, integritetsrådgivning, godkännande, blockering av publicering, granskning, avstämning, godkännande av undantag och tillämpning. Addressed by clauses [4.1.3; 4.2.5; 4.2.6; 4.3.6; 4.5.3; 4.5.4; 4.5.5; 6.1.1; 6.1.2; 9.1.3; 10.1.2].
- 13.3.6 **Article 26** - Mappas till publik ansvarsfördelning och kontaktinformation vid gemensamt personuppgiftsansvar i integritetsmeddelanden. Addressed by clauses [4.1.5; 4.2.1; 4.2.4].
- 13.3.7 **Article 28** - Mappas till stöd från personuppgiftsbiträden och underbiträden för personuppgiftsansvarigs skyldigheter avseende meddelanden, kundinformation för stöd till meddelanden och eskalering av motstridiga stödbegäranden. Addressed by clauses [4.1.6; 4.1.7; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 5.1.6].
- 13.3.8 **Article 30** - Mappas till koppling mellan meddelanden och behandlingsregister, inklusive ändamål, kategorier, mottagare, bevarandereferenser, överföringsreferenser och poster om stöd från personuppgiftsbiträden. Addressed by clauses [4.1.4; 4.2.2; 4.2.3; 4.5.4; 4.6.1; 7.1.5].

13.4 ISO/IEC 29100:2020

- 13.4.1 **Clause 5.3; Clause 5.8; Clause 5.10** - Mappas till ändamålsspecificering, öppenhet, transparens, meddelanden och ansvarsskyldighet genom REG02-kopplade meddelandeändamål, tydligt meddelandeinnehåll, publiceringskontroller, utlösare för ändringar av meddelanden och evidensbaserad granskning. Addressed by clauses [4.1.4; 4.2.2; 4.2.3; 4.2.7; 4.4.1; 4.4.2; 4.4.3; 4.5.1; 4.5.4; 4.5.6; 8.1.1].

13.5 ISO/IEC 29151:2022

- 13.5.1 **Annex A.9.1; Annex A.9.2** - Mappas till innehåll i integritetsmeddelanden, presentation på tydligt språk, tillgänglighet, publicering vid insamlingspunkten, utlösare för uppdatering av meddelanden och öppenhet om integritetspraxis. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.7; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.5.3].

13.6 ISO/IEC 29184:2020

- 13.6.1 **Clause 5.1; Clause 5.2; Clause 5.3** - Mappas till meddelandets syfte, tillhandahållande av meddelande, tydlig utformning, flerspråkig presentation och innehållselement för meddelanden online eller jämförbara meddelandekanaler. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.7; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4].