Graphic Packaging INTERNATIONAL	**Referanse:** CI- XX
Globale retningslinjer for personvern **KONSERNINSTRUKSER**	**Sist utstedt:** 1. mars 2024 **Gjenutstedt:** XX.XX.XXXX **Gyldig fra:** 1. mars 2024

Innholdsfortegnelse

Erklæring om retningslinjene

Graphic Packaging skal beskytte ansattes og kunders personopplysninger. Disse retningslinjene for personvern inneholder følgende informasjon, som skal sikre åpenhet og samsvar med globale personvernlover:

- hvilke typer personopplysninger Graphic Packaging samler inn
- hvorfor Graphic Packaging samler inn disse personopplysningene
- hvordan personopplysningene brukes og behandles
- dine rettigheter og valgmuligheter når det gjelder personopplysninger
- beskyttelse av personopplysninger
- kontaktinformasjon i forbindelse med personvern

Virkeområde

Disse retningslinjene gjelder for alt og alle Graphic Packagings personell, steder og annen eiendom globalt, blant annet:

- alle Graphic Packagings divisjoner, avdelinger og funksjoner
- alle Graphic Packagings underleverandører, konsulenter og andre tredjeparts tjenesteleverandører, unntatt der det er angitt medarbeiderspesifikke krav
- alle Graphic Packagings leasede eller egeneide fasiliteter der Graphic Packaging driver næringsvirksomhet
- all Graphic Packagings teknologi og nettverksinfrastruktur, heriblant informasjonssystemer, programmer, systemplattformer og dataoperasjoner som benyttes i den daglige driften av Graphic Packaging

Visse retningslinjer som det er henvist eller koblet til her, er interne og bare tilgjengelige for visse ansatte. Hvis du er ansatt og ikke får tilgang til retningslinjer det er koblet til her, kan du ta kontakt med law.department@graphicpkg.com og be om et eksemplar.

Viktige begreper

En «**registrert**» er en fysisk, levende person med personopplysninger som er, eller skal bli, behandlet.

«**Personopplysninger**» består av all informasjon som er forbundet med en identifisert eller identifiserbar fysisk person, for eksempel en ansatts navn og ansettelsesdokumentasjon, en kunderepresentants navn og kontaktopplysninger, en leverandørs navn og kontaktopplysninger samt data som er forbundet med visningspreferansene til personer som besøker nettstedet vårt.

«**Behandling**» er et svært bredt begrep som i utgangspunktet omfatter alt som gjøres med personopplysninger (heriblant enkel innsamling, lagring, tilgang til eller sletting av personopplysninger).

Behandling av personopplysninger

Graphic Packaging skal ha gjennomsiktige metoder for behandling av personopplysninger. Personer skal informeres om hvilke personopplysninger som samles inn, hvorfor de samles inn og hvordan de skal brukes, ved hjelp av tydelige personvernmerknader og samtykkemekanismer. Personopplysninger kan bare samles inn til spesifikke, uttrykkelige og berettigede formål, og kan ikke behandles utover det tiltenkte formålet. Endringer i formål er bare tillatt med samtykke fra personen det gjelder, eller hvis loven tillater det.

Graphic Packaging samler inn personopplysninger som er nødvendige for de erklærte formålene, og unngår å samle inn overflødige eller irrelevante opplysninger. Prosesser for datainnsamling skal inneholde tilstrekkelige sikkerhetstiltak for å beskytte dataene mot uautorisert tilgang, utlevering, endring og sletting.

Dataminimering, innebygd personvern og sensitivitetsreduserende tiltak

Personvernet til en enkeltperson ivaretas best ved å unngå å samle inn personopplysningene hans/hennes i det hele tatt. Behandling av personopplysninger som Graphic Packaging har i sin besittelse, må være helt nødvendig for det tiltenkte formålet, og vi skal bare samle inn den mengden som er strengt nødvendig for formålene med behandlingen. Vi skal med andre ord ikke samle inn personopplysninger vi ikke trenger.

Graphic Packaging har også et uttalt mål om å implementere nye programmer, tjenester og produkter basert på prinsippene for innebygd personvern og personvern som standardinnstilling. Innebygd personvern betyr at det tas hensyn til personvernet fra starten av og gjennom hele livsløpet til systemer, tjenester, produkter, funksjoner og prosesser. Dette krever proaktiv bruk av teknologiske nyskapninger og risikoidentifikasjon og -reduksjon i planleggings- og utformingsfasen, samt kontinuerlige gjennomganger og nye vurderinger. Innebygd personvern innebærer at alle nye IT-systemer, tjenester, produkter og metoder i vår organisasjon konfigureres med fokus på å ivareta personvernet. Dette betyr at registrerte ikke behøver å gjøre noe ekstra for å beskytte personvernet sitt, og at standardinnstillingene i de aktuelle systemene skal være konfigurert slik at de gir best mulig beskyttelse.

Graphic Packaging skal også minimere risikoen for dataeksponering ved å redusere sensitiviteten til informasjonen som lagres, hvis mulig, ved å gjøre følgende:

- Redusere presisjonen til dataene som lagres, etter at de er samlet inn. Hvis for eksempel en kundes telefonnummer er brukt til statistisk analyse, skal bare en del av sifrene oppbevares, gjerne retningsnummeret.

- Konvertere personopplysningene til et mindre sensitivt format. Hvis for eksempel en kundes IP-adresse er brukt til å fastslå sted for statistisk analyse, skal IP-adressen

slettes etter at den er koblet til en by eller et tettsted.

- Begrense tilgangen til store mengder personopplysninger. Ansatte som trenger tilgang til individuelle personopplysninger, trenger for eksempel ikke automatisk tilgang til grupperte personopplysninger.

Lagring av behandlingsdokumentasjon

Visse lover og forskrifter krever at Graphic Packaging lagrer korrekt dokumentasjon på hvordan og hvorfor personopplysninger brukes, lagres og behandles (denne dokumentasjonen på behandling og prosessen med å generere dem, kalles også *datakartlegging*). Dokumentasjonen på behandlingsaktiviteter skal blant annet inneholde hvilke kategorier av personopplysninger som behandles, en liste over relevante leverandører og tjenesteleverandører som brukes, hvilke formål personopplysningene brukes til, og eventuelle overføringer av personopplysninger til utlandet (for eksempel til leverandører i andre land). Datakartlegging er en grunnplikt i EUs og Storbritannias generelle personvernforordning (GDPR). Personvernlovene i visse delstater i USA krever generelt også at organisasjoner som Graphic Packaging klarer å påvise hvordan de bruker personopplysninger, og datakartlegging er en enkel måte å oppfylle dette kravet på. Graphic Packaging skal opprettholde et korrekt, oppdatert og utfyllende datakart.

Vurderinger av personvernkonsekvenser (Data Protection Impact Assessments – DPIA) og risiko

Målet med Graphic Packagings personvernprogram er å styre og redusere personvernrisiko. Personvernrisiko handler om hvilke konsekvenser det får for en enkeltperson at Graphic Packaging behandler personopplysningene hans/hennes. Dette inngår i en større risikovurdering for Graphic Packaging.

Graphic Packaging gjennomfører personvernvurderinger (Privacy Impact Assessments – PIA) eller vurderinger av personvernkonsekvenser (DPIA) for å oppnå åpenhet og kontroll i jurisdiksjoner der dette kreves. En PIA eller DPIA gjennomføres som en del av sjekklisten for innføring i prosjektkalenderen, når Graphic Packagings retningslinjer krever det eller hvis det følger av rettslige krav eller krav om samsvar.

Begrepene PIA og DPIA brukes ofte om hverandre, men DPIA gjelder vanligvis en spesifikk rettslig plikt i personvernforordningen (GDPR) som gjelder i EU og Storbritannia, mens PIA ofte er en generell vurdering av personvernrisiko som enten utføres i tråd med en annen personvernlov eller som foretrukket metode i et personvernprogram. Hos Graphic Packaging bruker vi begrepet PIA om den innledende risikovurderingen som utføres i samsvarsportalen OneTrust, og resultatet av denne avgjør om det er nødvendig å gjennomføre en fullstendig DPIA.

Det er ikke obligatorisk å gjennomføre en DPIA for alle prosjekter Graphic Packaging setter i gang. Loven krever en DPIA hvis et prosjekt sannsynligvis vil medføre høy risiko for enkeltpersoners rettigheter og friheter, særlig ved anvendelse av ny teknologi.

En DPIA er derfor i alt vesentlig en risikovurdering, der det skal tas hensyn til behandlingens art, omfang, sammenheng og formål, og den skal gjennomføres forut for behandlingen av personopplysninger. Uansett om et spesifikt Graphic Packaging-prosjekt er internt eller om det er en prosess, et produkt eller et system som leveres av en tredjepart, skal DPIA-vurderingen settes i gang så tidlig som praktisk mulig under anskaffelsen eller utformingen av prosjektet, selv om noen av aspektene ved prosjektet fremdeles er uvisse.

Les mer i Graphic Packagings **DPIA Policy and Procedure** (retningslinjer og prosedyre for DPIA) her: Data Privacy Impact Assessment Policy (retningslinjer for vurdering av personvernkonsekvenser (Data Privacy Impact Assessment – DPIA))

Rettsgrunnlag for behandling av personopplysninger

Graphic Packaging har bare anledning til å behandle personopplysninger med gyldig rettsgrunnlag. Det finnes flere aktuelle rettsgrunnlag for behandling av personopplysninger. Det er viktig å fastslå hvilket rettsgrunnlag som skal benyttes, før behandlingsaktiviteter settes i gang.

Personvernmerknader vil angi rettsgrunnlaget for behandling av personopplysninger for bestemte formål. Graphic Packaging skal også dokumentere beslutningen om hvilket rettsgrunnlag som gjelder for spesifikke behandlingsaktiviteter, for å kunne påvise samsvar med gjeldende personvernlover og -forskrifter.

Typiske rettsgrunnlag for behandling av personopplysninger omfatter følgende:

- Samtykke: Når personen (den registrerte) har gitt tydelig samtykke til behandling av personopplysningene for et spesifikt formål. Samtykket skal være avgitt skriftlig eller i et annet lovlig format, og personen skal være informert på forhånd om formålet med behandlingen av personopplysninger og en eventuell overføring. Samtykkeerklæringen skal fremheves spesielt når den inkluderes som en del av andre erklæringer, for at den skal være tydelig for personen.

- Kontrakt: Når behandlingen er nødvendig på grunn av en kontrakt Graphic Packaging har inngått med en annen organisasjon eller person.

- Rettslig plikt: Når behandlingen av personopplysninger er nødvendig for at Graphic Packaging skal kunne oppfylle krav i lov (dette omfatter ikke kontraktforpliktelser).

- Berettiget interesse: Når behandlingen av personopplysninger er nødvendig av hensyn til Graphic Packagings eller en tredjeparts berettigede interesse, med mindre det er gode grunner til å beskytte enkeltpersoners personopplysninger, som veier tyngre enn den berettigede interessen.

Datasikkerhet

Konfidensialitet og autorisasjon

Bare autorisert personell hos Graphic Packaging som har plikt til å etterleve kravene om datakonfidensialitet, har tillatelse til å behandle personopplysninger. Det er forbudt for dem å bruke personopplysninger til egne, private formål, overføre personopplysninger til uautoriserte parter eller på urettmessig vis gjøre dem tilgjengelige for uautoriserte personer.

Begrepet «uautoriserte» omfatter, i denne sammenhengen, ansattes tilgang til, eller bruk av, personopplysninger når formålet ikke er å utføre arbeidsoppgavene sine. Konfidensialitetsplikten gjelder også etter at ansettelsesforholdet har opphørt.

Kryptering og pseudonymisering

Anonymisering eller pseudonymisering av personopplysninger brukes på et tidlig stadium, hvis mulig, såfremt kostnadene er rimelige i forhold til det tiltenkte beskyttelsesformålet.

Pseudonymisering oppnås gjennom et balansert sett med tiltak, inkludert maskering (statisk og/eller dynamisk), tokenisering og/eller kryptering.

Regelmessige sikkerhetskontroller og -tester

Graphic Packaging gjennomfører regelmessige sikkerhetskontroller og -vurderinger for å avdekke sårbarheter, vurdere risikoer og styrke sikkerhetstiltak. Penetrasjonstesting og sårbarhetsskanning utføres for proaktivt å avdekke og eliminere potensielle sårbarheter når det gjelder sikkerhet. Les mer i **Audit and Compliance Assessment Policy** (retningslinjer for kontroll og samsvarsvurdering) her: Audit and Compliance Assessment Policy (retningslinjer for kontroll og samsvarsvurdering)

Overvåking

Graphic Packaging forbeholder seg rett til å overvåke e-post- og nettrafikk i den utstrekning loven tillater det. Les mer i **Acceptable Use of Assets Policy** (retningslinjer for akseptabel bruk av selskapets eiendom) her: Acceptable Use of Assets Policy (retningslinjer for akseptabel bruk av selskapets eiendom)

Sosiale medier

Graphic Packaging er innforstått med at ansatte er aktive i sosiale medier. Graphic Packaging forbeholder seg rett til å overvåke aktiviteter i sosiale medier i den utstrekning lover tillater det, men skal også ivareta de ansattes personvern der det er mulig. Les mer i Graphic Packagings **Acceptable Use of Social Networking Policy** (retningslinjer for akseptabel bruk av sosiale nettverk) her: Acceptable Use of Social Networking Policy (retningslinjer for akseptabel bruk av sosiale nettverk)

Administrasjon av mobilt utstyr

Ansatte hos Graphic Packaging bruker mobilt utstyr som mobiltelefoner og nettbrett. Graphic Packaging skal beskytte personopplysninger der det er mulig, og såfremt bruk av slikt utstyr er tillatt av personlige årsaker. Les mer i følgende retningslinjer:

- **Asset Management Policy** (retningslinjer for håndtering av selskapets eiendom) er tilgjengelige her: Asset Management Policy (retningslinjer for håndtering av selskapets eiendom)
- **Mobile Computing Security Policy** (retningslinjer for sikkerhet ved bruk av mobilt utstyr) er tilgjengelige her: Mobile Computing Security Policy (retningslinjer for sikkerhet ved bruk av mobilt utstyr)
- **Personally Owned Devices Policy** (retningslinjer for privateid utstyr) er tilgjengelige her: Personally Owned Devices Policy (retningslinjer for privateid utstyr)

Datalagring

Jo lenger personopplysninger lagres, desto høyere er sannsynligheten for utilsiktet utlevering, tap, tyveri og/eller at opplysningene foreldes. Tid er med andre ord en stor risikofaktor for datasikkerhetsbrudd. Graphic Packaging har som mål å bare lagre personopplysninger så

lenge som nødvendig for å oppfylle formålet eller rettslige krav.

Personopplysninger som Graphic Packaging lagrer, håndteres i samsvar med programmet for dokumentstyring, som fastlegger hvor lenge og hvorfor dataene lagres, samt hvordan de kan fjernes fra alle datalagre.

Les mer i Graphic Packagings **Records Management Program Policy** (retningslinjer for dokumentstyring) her: Records Management Program Policy (retningslinjer for dokumentstyring)

Registrertes rettigheter

Graphic Packaging skal opprettholde de høyeste standarder for databeskyttelse og personvern. Et viktig aspekt ved Graphic Packagings åpenhet og ansvar er å etterleve, anerkjenne og respektere de registrertes rettigheter slik de er skissert i gjeldende personvernlover og -forskrifter.

Særlige kategorier og sensitive personopplysninger

Særlige kategorier av personopplysninger kan inneholde informasjon som avdekker etnisk opprinnelse, seksuell legning, politiske oppfatninger, religiøs tro eller livssyn, statsborgerskap og immigrasjonsstatus, fagforeningsmedlemskap og data om helse eller sexliv. Slike sensitive personopplysninger defineres og håndteres i samsvar med gjeldende lokale personvernlover.

I lys av sammenheng og nedslagsfelt, volum og tiltenkt bruk kan andre behandlingsaktiviteter hos Graphic Packaging også regnes som sensitive, etter at personvernrisikoen er vurdert. Finansinformasjon i forbindelse med Graphic Packagings lønnsadministrasjon krever for eksempel ytterligere vern og sikkerhetskontroller.

Les mer om dataklassifikasjon i **Information Classification Policy** (retningslinjer for informasjonsklassifikasjon) her: Information Classification Policy (retningslinjer for informasjonsklassifikasjon)

Datadeling og tredjeparter

Graphic Packaging kan inngå en kontrakt med en tredjepart om innsamling, lagring og behandling av data, heriblant personopplysninger. Tredjeparten kan levere tjenester som drifting, bortsetting eller private eller offentlige skytjenester.

Hvis Graphic Packaging vil inngå en kontrakt med en tredjepart om behandling av personopplysninger, må kontrakten kontrolleres av IT-prosjektledelsen før den gjennomføres. Når tredjeparten er godkjent som behandler, skal forholdet til tredjeparten reguleres i en skriftlig avtale der Graphic Packagings og underleverandørens rettigheter og plikter er spesifisert. Det skal velges en underleverandør som garanterer de teknologiske og organisatoriske sikkerhetstiltakene som kreves i disse retningslinjene for personvern, og som gir tilstrekkelige garantier for vern av personopplysninger og de registrertes utøvelse av sine rettigheter.

Underleverandøren må være kontraktsforpliktet til utelukkende å behandle personopplysninger innenfor omfanget av kontrakten og instruksene fra Graphic Packaging. En personvernavtale som er godkjent av juridisk avdeling, skal være vedlagt alle kontrakter

som gjelder behandling av personopplysninger. Personopplysninger skal ikke behandles for andre formål. Graphic Packaging er alltid ansvarlig for personopplysningene som behandles av kontraktøren.

Varsling om datasikkerhetsbrudd

Alle medarbeidere hos Graphic Packaging og kontraktøren har ansvar for å hindre datasikkerhetsbrudd i forbindelse med personopplysninger. I tillegg oppfordres alle til å varsle den juridiske rådgiveren som har ansvaret for personvernsaker, eller personvernombudet i bestemte geografiske områder, om uregelmessigheter i forbindelse med behandlingsaktiviteter knyttet til personopplysninger.

Retningslinjer for betimelig avdekking, respons, behandling og varsling (av både tilsynsmyndigheter og potensielt de berørte enkeltpersonene) er skissert i Graphic Packagings **Data Breach Response Policy** (retningslinjer for respons på datasikkerhetsbrudd), som er tilgjengelige her: Data Breach Response Policy (retningslinjer for respons på datasikkerhetsbrudd)

Se også **Security Incident Response Policy** (retningslinjer for respons på sikkerhetshendelser), som er tilgjengelige her: Security Incident Response Policy (retningslinjer for respons på sikkerhetshendelser)

Internasjonal dataoverføring

Personopplysninger som overføres innenfor eller utenfor organisasjonen, overføres på en trygg måte ved bruk av godkjente protokoller og sikre kanaler. Graphic Packaging oppfyller relevante rettslige og regulatoriske krav til internasjonal dataoverføring, og sikrer at det brukes korrekte, gyldige mekanismer for dataoverføring før personopplysninger overføres internasjonalt. Dette innebærer å sikre at Graphic Packaging inngår kontrakter i samsvar med gjeldende personvernlover og -forskrifter med alle tredjeparts underleverandører og tjenesteleverandører som eventuelt skal behandle personopplysninger på Graphic Packagings vegne.

Samsvar med lover og forskrifter

Graphic Packagings virksomhet er i samsvar med relevante internasjonale, nasjonale og lokale lover og forskrifter som regulerer behandling og beskyttelse av personopplysninger, blant annet GDPR i EU, GDPR i Storbritannia, den generelle personvernloven i Brasil og føderale og delstatlige personvernlover i USA.

Opplæring, bevisstgjøring og gjennomføring

Graphic Packaging skal sikre at de generelle prinsippene som er fastlagt i disse retningslinjene for personvern, etterleves. I denne forbindelse skal ledelsen hos Graphic Packaging påse at retningslinjene implementeres, med særlig vekt på å opplyse ansatte om retningslinjene.

Ansatte har også plikt til å erklære at de forstår og skal følge disse retningslinjene for personvern.

Hvis det er behov for ytterligere opplæring, skal det rettes en forespørsel til personvernkomiteen. Når det informeres om retningslinjene, skal det også gis en påminnelse om at brudd på de generelle prinsippene i retningslinjene for personvern under visse omstendigheter kan få rettslige konsekvenser, for eksempel strafferettslige bøter, erstatningsansvar og følger for ansettelsesforholdet.

Personvernombud (Data Protection Officer – DPO)

Graphic Packaging har valgt et globalt personvernombud, som skal føre tilsyn med og sikre at personvernlover og -forskrifter etterleves. Der det er aktuelt eller nødvendig, har Graphic Packaging i tillegg valgt lokale personvernombud i samsvar med lokale krav. Personvernombudenes kontaktinformasjon, heriblant fullt navn, stilling og kontaktopplysninger, er tilgjengelig slik at enkeltpersoner kan ta kontakt med spørsmål eller henvendelser som gjelder personvern. Personvernombudet samarbeider med ledelse, ansatte og relevante interessenter for å sikre en helhetlig tilnærming til personvern i hele organisasjonen, og fungerer som kontaktpunkt for henvendelser som gjelder personvern hos Graphic Packaging.

Versjonskontroll

Dato	Beskrivelse av endring	Forfatter
XX	XX	XX