Friskrivningsklausul: Denna globala policy har översatts med maskinöversättning. I händelse av en konflikt mellan den engelska originalversionen och denna översatta version ska den engelska versionen ha företräde.

Getinges globala policy

Datasekretess global policy

Dokumentägare	Anna Romberg
Version	v3
Antagen av styrelsen	26 april 2023

1. Sammanfattning

Syftet med denna Globala Datasekretesspolicy (“ **Global Policy** ”) är att ange de viktigaste datasekretesskraven och ge Getinges ledning, anställda och konsulter riktlinjer i deras dagliga arbete som involverar Behandling av Personuppgifter.

Getinge förbinder sig att behandla personuppgifter i enlighet med tillämpliga dataskyddslagar och förordningar. Sekretess ska alltid ha högsta prioritet i vår dagliga verksamhet.

Denna globala policy gäller alla anställda, styrelseledamöter och affärspartners som agerar på uppdrag av Getinge.

2. Definitioner

I denna globala policy har följande termer följande betydelse:

Datakontrollant	En juridisk person som ensam eller tillsammans med andra enheter bestämmer ändamålen och medlen för behandlingen av personuppgifter.
Databehandlare	En juridisk person som behandlar personuppgifter på uppdrag av en personuppgiftsansvarig.
Dataskyddskonsekvensbedömning	En systematisk process för att utvärdera ett projekt, en process eller en lösning med avseende på dess inverkan på dataskyddet.
Dataskyddslagar	Alla tillämpliga dataskyddslagar och förordningar, inklusive men inte begränsat till GDPR.
Registrerad	Den enskilda person som personuppgifterna avser.
GDPR	Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd

	för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/ EC.
Personlig information	All information som rör en registrerad. En registrerad är en person som kan identifieras, direkt eller indirekt, med hjälp av ett namn, ett identifikationsnummer, platsdata, en onlineidentifierare eller faktorer som är specifika för den fysiska, fysiologiska, genetiska, mentala, ekonomiska, kulturella eller sociala identiteten hos den fysiska personen. person. Personuppgifter inkluderar även kontaktuppgifter till anställda, såsom e-postadresser och kontaktpersoner på jobbet.
Personuppgiftsintrång	Ett säkerhetsbrott som leder till oavsiktlig eller olaglig förstörelse, förlust, ändring, obehörigt avslöjande av eller tillgång till Personuppgifter som överförs, lagras eller på annat sätt behandlas.
Behandling av personuppgifter	Varje operation eller uppsättning operationer som utförs på personuppgifter eller på uppsättningar av personuppgifter, oavsett om det är automatiserat eller inte, såsom insamling, inspelning, organisation, strukturering, lagring, anpassning eller växling, hämtning, konsultation, användningsutlämnande genom överföring , spridning eller på annat sätt tillgängliggörande, anpassning eller kombination, begränsning, radering eller förstörelse. Behandlingen inkluderar även visning av personuppgifter.
Särskilda kategorier av personuppgifter -	Alla Personuppgifter som direkt eller indirekt indikerar en levande fysisk persons ras eller etniska ursprung, politiska åsikter, filosofiska eller religiösa övertygelser, sexuella läggning, fackföreningsmedlemskap och aktiviteter, genetiska eller biometriska data och data som rör hälsa eller sexliv.
Tillsynsmyndigheten	En oberoende offentlig myndighet som ansvarar för att övervaka efterlevnaden av dataskyddslagar.

3. Omfattning och målsättning

Denna globala policy gäller för alla Getinge-företag, dess dotterbolag och gemensamma verksamheter (gemensamt " **Getinge** ") och gäller alla våra anställda, samt konsulter och byråpersonal som arbetar i Getinges lokaler eller under ledning av Getinge (alla hänvisade till i denna globala policy som " **anställda** "). Den allmänna regeln är att denna globala policy gäller all behandling av personuppgifter inom Getinge. Undantag gäller endast i fall som anges i denna globala policy.

Målet med denna globala policy är att tillhandahålla:

a) Allmän kunskap om personuppgifter och gällande dataskyddslagar
b) Vägledning om de lagkrav som är av primär betydelse för Getinge
c) Krav på Getinge vid behandling av personuppgifter
d) Instruktioner som måste följas när Getinge behandlar personuppgifter

Med denna globala policy förbinder vi oss att skydda personuppgifter i enlighet med dataskyddslagar.

4. Användningsområde

Specifikt om tillämplighet

Denna globala policy gäller för:

a) Behandling av personuppgifter i affärsprocesser
b) IT-funktioner, lösningar eller tjänster som används för att behandla personuppgifter
c) Verktyg som Outlook, PowerPoint, Word och Excel
d) Situationer när Getinge tillhandahåller produkter eller tjänster som inkluderar behandling av personuppgifter på uppdrag av tredje part, t.ex. IT-lösningar som tillhandahålls sjukhus
e) Alla andra situationer när Getinge är antingen en personuppgiftsansvarig, databehandlare och/eller gemensam personuppgiftsansvarig enligt beskrivningen i denna globala policy

Andra krav än de som anges i denna globala policy kan vara nödvändiga för specifik verksamhet, såsom krav på IT-säkerhet. Utöver denna globala policy kan det finnas ytterligare instruktioner och riktlinjer för behandling av personuppgifter som är tillämpliga på specifika Getinge-team.

Tillämpliga lagar, lokala krav och avvikelser

Denna globala policy är baserad på europeiska dataskyddslagar och förordningar men är relevant och tillämplig för all Getinges behandling av personuppgifter även utanför EU/EES. Skälen till att europeiska dataskyddslagar och förordningar är tillämpliga på sådan behandling kan till exempel vara att:

a) Behandlingen avser rutiner, system, rutiner eller beslut fattade av Getinges huvudkontor, som är baserat inom EU/EES
b) Behandlingen avser varor och tjänster som erbjuds till registrerade inom EU/EES, eller övervakning av deras beteende
c) Enheten utanför EU/EES anses vara etablerad inom EU/EES på grund av till exempel att ha anställda inom EU/EES

När lokala dataskyddslagar och förordningar ställer krav som är andra eller strängare än de som ställs i denna globala policy, ska Getinge följa sådana lagar och förordningar. Om lagar och/eller förordningar strider mot denna globala policy ska det strängare kravet ha företräde. Kontakta Datasekretessteamet för ytterligare vägledning.

Anonymiserade och pseudonymiserade uppgifter

Denna globala policy gäller inte information som är *helt* anonym, dvs information som inte kan relateras tillbaka till en identifierbar individ. På grund av tekniska lösningar som finns tillgängliga på dagens marknad finns det många olika sätt att identifiera individer genom att använda rätt tekniska verktyg. Observera att anonymisering kan vara komplicerad att uppnå i praktiken.

Denna globala policy gäller för information som har genomgått så kallad pseudonymisering, det vill säga information som kan kopplas till en individ med hjälp av en annan uppsättning information (som en "nyckel"). Pseudonymiserade uppgifter betraktas fortfarande som personuppgifter.

NOTERA!

Personuppgifter anses inte vara anonymiserade när uppgifter som innehas av ett Getinge-företag i kombination med andra uppgifter som innehas av ett annat Getinge-företag eller en tredje part kan relateras till en individ. Till exempel betraktas såväl statiska som dynamiska IP-adresser som Personuppgifter eftersom IP-numret kan relateras till individer om det kombineras med information som finns hos internetoperatören. Det spelar ingen roll att Getinge inte kan komma åt den information som innehas av tredje part, det vill säga att den fortfarande betraktas som Personuppgift.

5. Ansvar för efterlevnad

Datasekretessteam

Getinges datasekretessorganisation och datasekretessteamet beskrivs i Data Privacy Governance-direktivet. Datasekretessteamet ska upprätthålla nödvändig expertkunskap inom datasekretessområdet.

Datasekretessteamet ska ses som en diskussionspartner inom Getinge och datasekretessteamets åsikt ska ges vederbörlig vikt i datasekretessfrågor.

Se vidare: Datasekretessstyrningsdirektivet

Getingebolags ansvar

Det är det yttersta ansvaret för varje Getinge-företag att följa lagar, förordningar, interna Getinge-beslut, processer och procedurer som beskrivs i denna globala policy. Se även avsnitt 19 angående roller och ansvar.

Rapportera risker

Getinge ska sträva efter att fullt ut följa alla dataskyddslagar och att proaktivt ta itu med och korrigera affärspraxis som leder till, eller potentiellt kan leda till, överträdelser. Varje anställd

uppmuntras och förväntas rapportera alla incidenter eller misstankar om bristande efterlevnad, med försäkran om att det inte kommer att bli några repressalier eller andra negativa konsekvenser för personer som agerar i god tro. Anställda förväntas ta upp farhågor om datasekretessrisker och/eller misstänkt bristande efterlevnad till datasekretessteamet. Det kan också alltid tas upp betänkligheter enligt 18 §.

6. Allmänna krav när Getinge-företag behandlar personuppgifter som personuppgiftsansvarig eller Joint Controller

Kontroller

När ett Getinge-företag behandlar personuppgifter kan det göra det på eget initiativ, och avgöra varför och hur personuppgifterna kommer att behandlas. Om ett Getinge-företag bestämmer medlen (hur) och syftena (varför) för behandlingen av personuppgifter, kallas det för en personuppgiftsansvarig.

EXEMPEL

Om Getinge samlar in personuppgifter om sina anställda i syfte att betala ut löner varje månad, fastställer Getinge ändamålen och medlen för behandlingen och anses därför vara personuppgiftsansvarig för behandlingen av personuppgifter.

Joint Controller

Under vissa omständigheter kan två eller flera personuppgiftsansvariga gemensamt bestämma syftet (varför) och medel (hur) för behandlingen av personuppgifter. Till exempel kan ett Getinge-företag dela rollen som datakontrollant med en eller flera interna och/eller externa enheter. Detta kallas gemensamt kontrollansvar.

När det finns ett gemensamt personuppgiftsförhållande finns det ett lagkrav på att ingå ett gemensamt personuppgiftsbiträdesavtal för att fastställa de personuppgiftsansvarigas respektive ansvar. Getingeföretaget ska säkerställa att tillämplig mall som finns tillgänglig på intranätet används.

EXEMPEL

Om ett Getingeföretag genomför en forskningsstudie tillsammans med ett sjukhus, där Getingeföretaget och sjukhuset i samverkan bestämmer varför och hur personuppgifter ska behandlas inom projektet, kan Getingeföretaget och sjukhuset betraktas som gemensamma registeransvariga och skulle i ett sådant fall behöver ingå ett gemensamt controlleravtal.

Grundläggande krav för insamling och behandling av personuppgifter

Personuppgifter får endast behandlas för specificerade, uttryckliga och legitima ändamål. För att ändamålen ska anses vara legitima måste den planerade behandlingen, oavsett om en registrerad person har lämnat samtycke till behandlingen:

a) Har ett legitimt affärssyfte och får inte bryta mot några dataskyddslagar eller andra lagar;
b) Var proportionell och nödvändig för att uppfylla syftena;

c) Inte användas på sätt som har omotiverade negativa effekter på de registrerade; och
d) Hantera de registrerades personuppgifter endast på sätt som de registrerade rimligen kan förvänta sig.

All behandling av personuppgifter måste vara nödvändig för att uppnå syftet med behandlingen och de registrerade får inte vilseledas eller vilseledas med avseende på syftet med eller omfattningen av behandlingen av deras personuppgifter. Personuppgifter får inte behandlas på något sätt som är oförenligt med de syften som har meddelats den registrerade. Vidare ska personuppgifter som behandlas av Getinge-företag vara korrekta och vid behov hållas uppdaterade.

Laglig grund för behandling av personuppgifter

Allmänt om rättslig grund

Getinge får endast behandla personuppgifter om minst något av följande gäller:

a) **Samtycke.** Den registrerade har lämnat ett förhandssamtycke till behandlingen för det eller de angivna ändamålen. Se nedan i detta avsnitt 6 angående samtycke och återkallande av samtycke.

b) **Laglig skyldighet.** Getinge måste Behandla Personuppgifterna för att uppfylla en rättslig skyldighet som Getinge är föremål för (såsom att lämna skatteinkomstuppgifter till skattemyndigheterna).

c) **Fullgörande av ett kontrakt.** Behandlingen av personuppgifter är nödvändig för att Getinge ska kunna fullgöra sina skyldigheter i ett avtal som det har ingått med den registrerade (såsom att behålla bankkontouppgifter för att betala löner enligt ett anställningsavtal).

d) **Getinges berättigade intresse.** Getinge kan komma att behandla personuppgifter för legitima ändamål som en del av sin verksamhet (såsom att hålla en databas med information om sina kunder eller affärspartners, eller samla in namn och telefonnummer till nödkontakter för sina anställda), utom där sådana intressen åsidosätts av den registrerades intressen eller grundläggande rättigheter och friheter. När denna rättsliga grund tillämpas måste det specifika intresset i fråga identifieras och den registrerade bör informeras om sådant.

e) **Övrig.** Det finns andra sällsynta skäl på vilka personuppgifter kan behandlas, nämligen skyddet av den registrerades vitala intressen eller uppgifter som utförs i allmänhetens intresse.

Samtycke och återkallande av samtycke

Samtycke bör endast användas av Getinge-bolag när ingen annan rättslig grund kan användas. Om samtycke tillämpas som rättslig grund måste ett Getingeföretag kunna visa att den registrerade har lämnat samtycke till Behandling av personuppgifter och att sådant samtycke är giltigt. Förkryssade rutor, tystnad eller inaktivitet utgör aldrig samtycke. Om så är lämpligt bör separata samtycken erhållas för olika ändamål med behandlingen.

Samtycket ska vara:

a) Ges utan att vara föremål för andra villkor;
b) Informerad (se nedan i detta avsnitt angående information till registrerade);
c) Tillhandahålls frivilligt (den registrerade får inte känna sig pressad att ge samtycke); och
d) Specifik och entydig (den registrerade måste vara medveten om omfattningen av samtycket).

Ett samtycke ska lämnas skriftligt eller elektroniskt. Det måste tydligt anges om en registrerad accepterar den föreslagna behandlingen av personuppgifter. Samtycke kan inte ges genom tystnad eller inaktivitet.

Den registrerade kan när som helst återkalla det lämnade samtycket. När samtycke återkallas ska det berörda Getinge-företaget upphöra med Behandlingen av personuppgifter om den registrerade i den mån behandlingen är baserad på samtycke. Detta innebär att alla Personuppgifter om den individ som har återkallat samtycket måste raderas eller anonymiseras, inklusive Personuppgifter i eventuella säkerhetskopior.

Ytterligare krav för behandling av särskilda kategorier av personuppgifter

Särskilda kategorier av personuppgifter, ofta kallade "Känsliga personuppgifter", ges särskilt skydd och bör inte behandlas av Getinge förutom under särskilda omständigheter.

Behandling av särskilda kategorier av personuppgifter får endast utföras om det finns en laglig grund för behandlingen enligt beskrivningen ovan i detta avsnitt 6. Dessutom får sådana uppgifter endast behandlas om minst ett av följande villkor är uppfyllt:

a) Den registrerade har gett uttryckligt samtycke till behandlingen för det eller de angivna ändamålen;
b) Behandlingen är nödvändig för att fullgöra skyldigheterna och utöva rättigheterna för den personuppgiftsansvarige eller den registrerade inom arbetsrättsområdet i den mån det är tillåtet enligt nationella lagar eller kollektivavtal;
c) Behandlingen är nödvändig för att upprätta, utöva eller försvara ett rättsligt anspråk; eller
d) Behandlingen är nödvändig för förebyggande eller arbetsmedicinskt syfte, för bedömning av arbetstagarens arbetsförmåga, medicinsk diagnos, tillhandahållande av hälso- och sjukvård eller behandling.

Getinge bör generellt undvika att behandla särskilda kategorier av personuppgifter och får endast göra det om något eller flera av ovanstående gäller. Lokala undantag kan också gälla.

NOTERA!

Uttryckligt samtycke innehåller kraven för ett regelbundet samtycke enligt beskrivningen ovan i detta avsnitt 6 angående samtycke och återkallande av samtycke. Dessutom ska individen tydligt presenteras för en möjlighet att samtycka till eller inte hålla med om den föreslagna behandlingen av personuppgifter.

Personuppgifter inom ramen för brott och fällande domar

Getinge ska inte behandla några personuppgifter som rör brott eller fällande domar, inklusive misstankar, förutom när det är tillåtet eller krävs enligt tillämpliga lagar och förordningar. Observera att det finns ett generellt förbud mot att behandla denna typ av personuppgifter. Undantag kan dock finnas i nationella lagar och förordningar.

Det kan finnas krav på olika Getinge-avdelningar att behandla personuppgifter relaterade till brott, fällande domar eller relaterade misstankar. Till exempel, i samband med utredningar och/eller due diligence finns det krav (där det stöds av tillämplig lag och förordning) på Legal, Compliance & Governance-avdelningen för att utföra faktainsamling, bakgrundskontroller av företag och/eller personal i relevanta befattningar.

NOTERA!

Datasekretessteamet ska alltid rådfrågas innan behandling av personuppgifter rörande brottsregister, brott, fällande domar eller relaterade misstankar.

Information till registrerade

Getinge ska ge de registrerade skriftligt meddelande med information om:

a) Namn och kontaktuppgifter för den enhet som är personuppgiftsansvarig;
b) Typerna av personuppgifter som behandlas och de relaterade ändamålen med behandlingen;
c) Den rättsliga grunden för behandlingen;
d) Hur länge personuppgifter kommer att sparas;
e) Mottagarna eller kategorierna av mottagare av personuppgifterna;
f) Information om den registrerades rättigheter enligt Avsnitt8 Nedan; och
g) Om tillämpligt:
    i. kontaktuppgifter till ansvarig dataskyddsombud;
    ii. varifrån personuppgifter har erhållits;
    iii. konsekvenserna om en registrerad inte tillhandahåller sina personuppgifter;
    iv. Getinges avsikter att överföra Personuppgifter utanför EU/EES i enlighet med Avsnitt9 Nedan; och
    v. Information om profilering.

Datasekretessteamet tillhandahåller mallar för sekretessmeddelanden som alltid ska användas när ett Getinge-företag behöver informera registrerade om behandling av personuppgifter. Mallarna innehåller ytterligare instruktioner om vilken information som ska lämnas till registrerade.

Det är varje Getinge-företags ansvar att säkerställa och visa att dess integritetsmeddelanden är tillräckliga och fullständiga och att de följer dataskyddslagarna. Dessutom ska Getinge-företag översätta integritetsmeddelanden till det lokala språket vid behov.

I förhållande till anställda lämnas information om Behandling av Personuppgifter vanligtvis i det Anställdas Integritetsmeddelande som de anställda får tillsammans med anställningsavtalet. Varje Getinge-företag ska se till att dess meddelande om anställdas integritet är lättillgängligt för de anställda och uppdaterat samt ger tillräcklig information om hur företaget behandlar personuppgifter om anställda.

Ändrade ändamål för behandling av personuppgifter

Innan ett Getinge-företag ändrar ändamålen för behandling av personuppgifter ska:

a) Bedöma lagligheten av Behandlingen av Personuppgifter och dokumentera bedömningen i enlighet med avsnitt 7 nedan;
b) Ge den registrerade skriftlig information som beskriver ändringarna av syftena med behandlingen; och
c) Om behandlingen är baserad på samtycke, skaffa ett nytt samtycke från den registrerade.

Profilering och automatiserat beslutsfattande

Allmänt om profilering

Profilering innebär varje form av automatiserad behandling av personuppgifter som inbegriper avsikten att utvärdera personliga aspekter relaterade till en registrerad eller förutsäga eller analysera den registrerades prestation på jobbet, ekonomiska situation, plats, hälsa, personliga

preferenser, intressen, tillförlitlighet eller beteende, förare beteende, kundbeteende, plats eller rörelse.

Profilering används ofta för att göra förutsägelser om individer genom att använda data från olika källor och göra statistiska avdrag. Syftet med behandlingen kan vara att analysera den registrerades egenskaper eller beteendemönster för att placera dem i en viss grupp eller kategori. Detta gör det möjligt för den personuppgiftsansvarige att göra förutsägelser om till exempel den registrerades intressen, förmåga att utföra en uppgift eller troligt beteende.

EXEMPEL

Profilering kan till exempel bestå av att analysera en individs beteende på webbplatser genom cookie-identifierare eller IP-adresser för att skicka personlig reklam om specifika produkter eller tjänster. Ett annat exempel på profilering gäller analys av tidigare köp för att förutsäga framtida köp. Därför är profilering en metod som ofta används i samband med direktmarknadsföring och sociala medier, men skulle också kunna användas för andra bearbetningsaktiviteter såsom i forskningsstudier.

Beslut utifrån profilering

Ett beslut som fattas av ett Getinge-företag baserat på profilering ska endast tillåtas när:

a) det är absolut nödvändigt för att ingå, eller för att fullgöra, ett avtal mellan den registrerade och den personuppgiftsansvarige (detta undantag bör tolkas snävt);
b) det är uttryckligen tillåtet enligt lag, inklusive för bedrägeri- och skatteflyktsövervakning och förebyggande syfte som utförs i enlighet med förordningar, standarder och rekommendationer från institutioner eller nationella tillsynsorgan, och för att säkerställa säkerheten och tillförlitligheten för en tjänst som tillhandahålls av Getinge; eller
c) den registrerade har gett uttryckligt samtycke.

Krav

Getinge-företag ska säkerställa följande när de engagerar sig i profilering:

a) Behandla endast nödvändiga personuppgifter för att uppfylla syftet;
b) Förse de registrerade med tillräcklig information om profileringen i enlighet med avsnitt 6. Om profileringen avser automatiserat beslutsfattande har de registrerade rätt att få en förklaring om det fattade beslutet samt information om rätten att invända mot sådant beslut;
c) Använd lämpliga matematiska eller statistiska procedurer för profileringen;
d) Genomför lämpliga tekniska och organisatoriska åtgärder i enlighet med avsnitt0 ; och
e) Säkra personuppgifter på ett sätt som tar hänsyn till de potentiella riskerna för de registrerades rättigheter och intressen och som bland annat förhindrar diskriminerande effekter mot individer på grundval av särskilda kategorier av personuppgifter eller som leder till åtgärder som har sådana effekt.

NOTERA!

Profilering ska godkännas i förväg av datasekretessteamet innan den genomförs.

Datalagring, lagring och radering av personuppgifter

Getinge-företag ska säkerställa att personuppgifter inte behandlas längre än:

a) nödvändiga i förhållande till syftet med behandlingen; och
b) tillåts enligt dataskyddslagar.

Getingebolag ska implementera bearbetade för att säkerställa att kraven i detta avsnitt uppfylls.

NOTERA!

Vissa länder (t.ex. Ryssland och Kina) kräver att alla Personuppgifter om dess medborgare lagras inom länets gränser. I andra länder kan det finnas krav på att lagra specifika Personuppgifter lokalt om de Behandlas för specifika ändamål (t.ex. Sverige kräver att bokföringsuppgifter lagras inom dess gränser). Lokaliseringskraven hindrar normalt inte Getinge från att även lagra en kopia av Personuppgifterna någon annanstans, om sådan lagring är nödvändig.

7. Bedömning och dokumentation av Bearbetning

Registrering av bearbetningsaktiviteter

När det krävs enligt dataskyddslagar är Getinge-företag ansvariga för att föra register över företagens behandlingsaktiviteter. Alla register ska förvaras i det efterlevnadsverktyg som valts och hanteras av datasekretessteamet. Mer information finns på sidan för datasekretess-intranät.

Kraven i detta avsnitt gäller både när Getinge-företag agerar som personuppgiftsansvariga och databehandlare.

Bedömning av laglighet innan en ny Bearbetningsaktivitet påbörjas

Innan man genomför en ny Behandlingsaktivitet eller gör ändringar i en pågående verksamhet ska Getingebolag bedöma lagligheten av Behandlingen av Personuppgifter och dokumentera bedömningen. Detta gäller även eventuella pågående Bearbetningsaktiviteter som tidigare inte har bedömts och/eller dokumenterats.

Kraven i detta avsnitt gäller både när Getinge-företag agerar som personuppgiftsansvariga och databehandlare.

Dataskyddskonsekvensbedömningar

Om Behandling av Personuppgifter sannolikt kommer att leda till en hög risk för de registrerades rättigheter och friheter, ska Getinge-företag, innan sådan planerad Behandling inleds, utföra en bedömning av Behandlingsverksamhetens inverkan på skyddet av Personuppgifter (Dataskyddskonsekvensbedömning). En dataskyddskonsekvensbedömning kan i synnerhet vara av relevans när Getinge-företag använder ny teknik och med hänsyn till Behandlingens art, omfattning, sammanhang och syften.

Dataskyddskonsekvensbedömningar ska alltid utföras av datasekretessteamet på uppdrag av ett Getinge-företag. Getingeföretaget ska samarbeta med Datasekretessteamet under bedömningen, inklusive men inte begränsat till att tillhandahålla nödvändig information.

8. Registrerad rättigheter

Hantering av förfrågningar från registrerade

Följande gäller för förfrågningar från registrerade:

a) Alla förfrågningar från registrerade ska omedelbart vidarebefordras till och hanteras av datasekretessteamet.
b) Registrerade personer får inte utsättas för negativa konsekvenser när de utövar registrerade rättigheter.
c) Alla förfrågningar från registrerade ska hanteras konfidentiellt.
d) Getinge-företag ska samarbeta med Datasekretessteamet för att Datasekretessteamet ska kunna svara på förfrågningar i tid.

Observera att den registrerades rättigheter inte är absoluta och att undantag kan gälla.

Processer för att hantera registrerades rättigheter

Getinge-företag är ansvariga för att implementera processer för att hjälpa datasekretessteamet med hanteringen av registrerades rättigheter att:

a) Begär tillgång till personuppgifter. Detta inkluderar de registrerades rätt att få information om behandlingen av personuppgifter som avser den aktuella individen och att säkerställa rätten till dataportabilitet.
b) Begär rättelse av felaktiga personuppgifter.
c) Begär radering av personuppgifter.
d) Invända när som helst mot Behandling av Personuppgifter när Behandlingen baseras på Getinges berättigade intresse, inklusive när Behandlingen avser profilering.
e) Skaffa begränsning av personuppgifter.

9. Överföringar av personuppgifter

Allmänt om överföringar

Personuppgifter ska endast överföras för att uppfylla ändamålen med behandlingen. Överföringar av personuppgifter inkluderar inte bara sändning av personuppgifter genom användning av elektroniska meddelanden såsom via e-post, utan inkluderar även när personuppgifter kan nås eller ses. Personuppgifter betraktas som överförda även om de endast är tillfälligt åtkomliga, ses eller på annat sätt behandlas.

EXEMPEL

Personuppgifter överförs när ett Getinge-företag i Frankrike lagrar personuppgifter i en mapp som kan nås av Getinge-anställda i Kina (se även i detta avsnitt 9 om överföring av personuppgifter från EU/EES till ett land utanför EU/EES).

Överföra personuppgifter från EU/EES till ett land utanför EU/E EA

Getingeföretag inom EU/EES ska som huvudregel inte överföra Personuppgifter utanför EU/EES. Sådana överföringar får endast göras om det är absolut nödvändigt.

Om överföringar av personuppgifter från länder inom EU/EES till länder utanför EU/EES är strikt nödvändiga ska Getinge-företag säkerställa att:

a) sådana överföringar är föremål för adekvata skyddsåtgärder i enlighet med dataskyddslagar, inklusive men inte begränsat till överföringar baserade på:
   i. Ett lämplighetsbeslut fattat av Europeiska kommissionen;
   ii. EU:s standardavtalsklausuler antagna av Europeiska kommissionen; eller
   iii. Uttryckligt samtycke.
b) en överföringskonsekvensbedömning har gjorts vid behov.

Före en överföring av personuppgifter har registrerade rätt att få information om överföringen och tillämpligt adekvat skydd i enlighet med avsnitt 6.

10. Dela och avslöja personuppgifter inom Getinge

Getinge-anställda och konsulter ska endast dela och avslöja personuppgifter till individer inom Getinge som behöver sådana uppgifter för att utföra arbetsuppgifter och där det finns ett legitimt affärssyfte för att dela eller avslöja sådana personuppgifter. Personuppgifter får endast delas eller avslöjas i den utsträckning det är nödvändigt för att uppfylla syftet med behandlingen. Personuppgifter får inte delas eller avslöjas eftersom det kan vara "trevligt att ha" för mottagaren.

11. Databehandlare

Allmänt om klausuler i avtal

Det är Getingebolagens ansvar att vid behov inkludera personuppgiftsklausuler och/eller databehandlingsavtal i Getinges standardaffärs- och anställningsavtal.

I de fall befintliga avtal redan finns ska Getinge-bolag uppdatera sådana avtal vid behov med personuppgiftsklausuler och/eller relaterade databehandlingsavtal.

NOTERA!

Databehandlaravtalsmallarna som finns på sidan Datasekretess-intranät bör alltid användas i de fall då ett databehandlaravtal krävs.

Getinge som databehandlare i förhållande till tredje part

Om ett Getingeföretag Bearbetar Personuppgifter på uppdrag av en tredje part (såsom en kund) ska Getinge och den tredje parten ingå ett databehandlingsavtal. Getingeföretaget ska säkerställa att tillämplig mall som finns tillgänglig på intranätet används.

EXEMPEL

Getinge agerar i de flesta fall som databehandlare i samband med tillhandahållande av våra mjukvarulösningar till sjukhus. Detta är fallet när Getinge behöver komma åt eller på annat sätt behandla personuppgifter när vi tillhandahåller mjukvarusupport. I dessa situationer kommer sjukhuset att fungera som datakontrollant.

Anlita en extern databehandlare

Om en tredje part kommer att behandla personuppgifter för Getinges räkning (t.ex. en leverantör) ska Getinge och tredje part ingå ett databehandlingsavtal. Getingeföretaget ska säkerställa att tillämplig mall som finns tillgänglig på intranätet används.

EXEMPEL

Om Getinge köper ett nytt IT-system/lösning som innefattar att leverantören av IT-systemet/lösningen behandlar personuppgifter för Getinges räkning (såsom lagring av personuppgifter och/eller tillgång till personuppgifter vid support) ska Getinge och leverantören gå in ingå i ett databehandlingsavtal. I denna situation är Getinge personuppgiftsansvarig och leverantören är databehandlare.

Getinge som databehandlare i förhållande till andra Getinge-bolag

Om ett Getinge-företag behandlar personuppgifter för ett annat Getinge-företags räkning, ska parterna ingå ett koncerninternt databehandlingsavtal. Getingebolagen/funktionerna ska säkerställa att:

a) den tillämpliga mallen som finns tillgänglig på sidan Datasekretess-intranät används; eller
b) ett koncerninternt databehandlingsavtal har redan ingåtts.

EXEMPEL

Om Getinge IT bistår Getinge HR med stöd som innefattar att Getinge IT behandlar personuppgifter på uppdrag av Getinge HR, ska ett koncerninternt databehandlaravtal ingås. I det här fallet är Getinge IT databehandlare och Getinge HR är datakontrollant.

12. Tekniska och organisatoriska säkerhetsåtgärder

Alla Getingebolag ska följa Getinges policyer och direktiv avseende informationssäkerhet. Getinge-bolagen ska också genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig för risken. Följande bör beaktas när sådana åtgärder genomförs:

a) Den senaste tekniken;
b) Kostnaden för genomförandet;
c) Behandlingens art, omfattning och syften; och
d) Risken för sannolikhet och allvarlighet för de registrerades rättigheter och friheter.

Det är varje Getinge-företags ansvar att säkerställa att Behandling av personuppgifter följer dataskyddslagstiftningen, inklusive att vidta lämpliga tekniska och organisatoriska åtgärder såsom åtkomsträttigheter, flaggning av personuppgifter för radering, automatisk radering och loggningsdata. När det gäller åtkomsträttigheter ska Getinge-företag säkerställa att åtkomst till

Personuppgifter speglar de anställdas och konsulternas roller, inklusive i fall av ändrade roller inom Getinge.

13. IT-lösningar Behandling av personuppgifter

Det är varje Getinge-företags ansvar att säkerställa att nya och befintliga IT-funktioner, lösningar och/eller tjänster som används för att behandla personuppgifter följer dataskyddslagar, inklusive men inte begränsat till krav gällande:

a) Integritet genom design och som standard;
b) Datalagring;
c) Begäran från den registrerade, inklusive dataportabilitet;
d) Tillräckliga tekniska och organisatoriska säkerhetsåtgärder; och
e) Åtkomsträttigheter.

Innan en ny IT-lösning används och innan ändringar görs i en befintlig IT-lösning ska Getinge-företag i god tid informera Datasekretessteamet om integritetsrisker, syften och de Personuppgifter som behandlas. Information ska också lämnas till Datasekretessteamet om behandling av personuppgifter i befintliga IT-lösningar.

Se vidare: Informationssäkerhetsdirektivet

14. Integritet genom design och som standard

Principerna för integritet genom design och som standard bör beaktas när Getinge utvecklar, designar, väljer och använder applikationer, tjänster och produkter som inkluderar Bearbetning av Personlig Pata. Dessa principer bör implementeras både vid tidpunkten för fastställandet av medlen för Behandling och vid tidpunkten för själva Bearbetningen.

Privacy by design är ett koncept och ett tillvägagångssätt för systemutveckling som tar hänsyn till dataskydd genom hela konstruktionsprocessen. Privacy by design fokuserar på att säkerställa att integritet är inbäddat i informationsteknologi, affärsprocesser, fysiska utrymmen och nätverksbaserade infrastrukturer från början.

Getinge bör se till att deras system och processer är speciellt utformade med dataskydd i åtanke. Dataskydd bör inte vara en eftertanke, utan inbyggt i strukturen för hur enheten bedriver sin verksamhet.

Sekretess som standard innebär att den personuppgiftsansvarige ska implementera mekanismer för att säkerställa att, som standard, endast nödvändiga personuppgifter behandlas för varje specifikt ändamål med behandlingen och särskilt inte samlas in eller bevaras utöver vad som är nödvändigt för dessa ändamål, både i termer av mängden data och lagringstiden. I synnerhet ska implementerade mekanismer säkerställa att personuppgifter som standard inte görs tillgängliga för ett obegränsat antal individer.

EXEMPEL

Som ett exempel skulle det vara relevant att överväga integritet genom design och som standard när Getinge bygger nya IT-system för lagring eller åtkomst av personuppgifter, utvecklar policyer

eller strategier som har konsekvenser för datasekretess, initierar delning av personuppgifter eller användning för nya ändamål.

Att designa projekt, processer, produkter eller system med integritet genom design och som standard i åtanke från början har flera fördelar, inklusive:

a) Möjligheten att identifiera potentiella problem i ett tidigt skede där det ofta är enklare och billigare att ta itu med dem.
b) Medvetenheten om datasekretess i hela organisationen ökar;
c) Sannolikheten att uppfylla skyldigheterna enligt dataskyddslagarna ökar och likaså minskar sannolikheten för överträdelser; och
d) Projekt, processer, produkter eller system är mindre benägna att vara integritetsintrång och ha en negativ inverkan på individer.

Speciellt när Getinge designar och utvecklar produkter och tjänster relaterade till personuppgifter, bör relevant information om hur Getinge ska följa integritetsskyddet och som standardkrav definieras.

15. Brott mot personuppgifter

Alla personuppgiftsintrång ska omedelbart rapporteras i enlighet med den process som beskrivs på sidan för dataskyddsintranät.

Getingebolagen ska:

a) säkerställa att alla lösningar som används för behandling av personuppgifter möjliggör rapportering av personuppgiftsintrång;
b) genomföra åtgärder som stödjer upptäckt av personuppgiftsintrång;
c) dokumentera omständigheterna kring ett personuppgiftsintrång, inklusive effekter, möjliga risker och vidtagna eller planerade åtgärder; och
d) samarbeta med datasekretessteamet när personuppgiftsintrång utreds och åtgärdas.

Se vidare: Personuppgiftsintrångsdirektivet

16. Tillsynsmyndigheter

Alla kontakter med tillsynsmyndigheter ska hanteras av Datasekretessteamet. Getingebolagen ska på begäran samarbeta med tillsynsmyndigheterna.

17. Avvikelser

Avvikelser från denna globala policy ska godkännas på samma behörighetsnivå som när den globala policyn ursprungligen godkändes.

18. Brott mot den globala policyn – Tala Upp

Tveka inte att ta upp en oro. Alla Getinge-anställda som misstänker brott mot denna globala policy förväntas ta upp frågan och ta upp frågan till sin linjechef, till Ethics and Compliance Office eller använda Getinges Speak Up Line. Getinge Speak Up Line är tillgänglig på Getinges interna och externa webbsidor. På Getinge accepterar vi inte någon form av vedergällning mot någon som uttalar sig, uttrycker oro eller åsikter.

Se vidare: Global Speak Up and Non Retaliation Directive

19. Roller och ansvar

Alla Getinge-anställda är individuellt ansvariga för att läsa, förstå och följa denna globala policy. Varje anställd är ansvarig för att agera i enlighet med denna globala policy.

Varje linjechef är ansvarig för att se till att varje teammedlem har tillgång till denna globala policy och relaterade direktiv, instruktioner och riktlinjer.

Dag-till-dag förstärkning, inklusive regelbunden information och utbildning inom området datasekretess, samt efterlevnadsuppföljning, är en del av varje chefs ansvar.

Brott mot denna globala policy kan leda till disciplinära åtgärder, upp till och inklusive uppsägning.

20. Vägledning och assistans

För att vägleda vårt agerande när det gäller Getinges ställningstaganden inom datasekretessområdet finns denna globala policy och flera direktiv och instruktioner. Om du har frågor om denna globala policy eller om du är osäker på vilka regler som gäller, vänligen kontakta datasekretessteamet.

21. Användbara länkar

Titel
Personuppgiftsintrångsdirektivet
Datasekretessstyrningsdirektivet
Direktivet om informationssäkerhet

Titel

Globalt Speak Up and Non-Retalie-direktiv