Ivoclar Vivadent koncernens dataskyddspolicy

Innehållsförteckning

1. Introduktion

Information är en värdefull resurs som utgör grunden för vår globala affärsverksamhet och hjälper oss att uppnå företagets målsättningar. Dagens informationsteknologier ger ökad tillgänglighet till information och även utökade möjligheter till hur denna kan användas genom kommunikationssystem i olika kanaler. Detta medför också ökade krav för hur företagen inom Ivoclar Vivadent koncernen (härefter också kallad “Ivoclar Vivadent” eller ”koncernen”) ska behandla information innehållande personuppgift för att detta ska stå i överensstämmelse med tillämplig lagstiftning samt för att minimera riskerna såväl för koncernens företag som för den person informationen rör.

2. Syfte

Denna dataskyddspolicy gäller för Ivoclar Vivadent koncernen och innehåller de regler för personuppgiftsskydd som ska implementeras inom vår företagsgrupp för att säkerställa tillräckligt skydd för de registrerade i enlighet med deras grundläggande rättigheter och friheter.

Genom denna dataskyddspolicy erkänner Ivoclar Vivadent sitt ansvar för att behandla personuppgifter som rör dess anställda, kunder, leverantörer, affärspartners och andra eventuella parter enligt gällande regler. Vi vill också understryka att vi genomgående i alla aspekter av vår affärsverksamhet anstränger oss för att upprätthålla en tillräcklig nivå av personuppgiftsskydd.

I denna dataskyddspolicy fastställs ramarna för utbyte av personuppgifter inom koncernen och efterlevnad är därför en förutsättning för att detta sker på ett lagligt sätt. Att denna policy följs säkerställer en adekvat dataskyddsnivå för gränsöverskridande överföring av personuppgifter i enlighet med tillämplig dataskyddslagstiftning.

3. Tillämpningsområde

Denna policy gäller för alla dotterbolag och andra närstående företag som faller inom Ivoclar Vivadent koncernens ansvarsområde, oavsett var någonstans de bedriver sin verksamhet.

Ivoclar Vivadent är baserat i Lichtenstein men har dotterbolag och andra närstående företag som bedriver verksamhet världen över. Detta innebär att EU-lagstiftning såväl som nationell lagstiftning i USA och andra länder är tillämplig för den information avseende anställda, kunder, leverantörer och andra som vi behandlar.

Tillämplig nationell och internationell lagstiftning har företräde över denna policy. I det fall att personuppgifter rörande personer som bor utanför EU hanteras av ett dotterbolag (eller annat närstående företag) eller på ett ställe som koncernen är ansvarig för och det utifrån personens bosättning föreligger skyldigheter enligt tillämplig nationell eller internationell lagstiftning har detta företräde över denna policy. Detta kan inkludera, men är inte begränsat till, vad som framkommit enligt tidigare riktlinjer från ansvariga tillsynsmyndigheter i fall där behandling bedöms vara extra riskfylld utifrån den registrerades grundläggande rättigheter och friheter.

I det fall att det helt saknas lagstadgade skyldigheter eller dessa inte är lika långtgående ska denna dataskyddspolicy gälla som en obligatorisk miniminivå för personuppgiftsskydd inom koncernen. Denna policy ska dock inte tolkas eller förvrängas på något sätt så att den ger en person större individuella rättigheter än vad som skulle gälla enligt tillämplig lagstiftning och andra bindande överenskommelser.

4. Definitioner

Tillämplig lagstiftning är de lagar som gäller inom den jurisdiktion under vilken den personuppgiftsansvarige faller inklusive alla lagar, föreskrifter och eventuella andra regler i sekundär lagstiftning.

Anonymisering syftar på ett villkor som ställs under behandlingen som avlägsnar kopplingen till en viss person så att denna inte längre kan identifieras eller endast identifieras genom ett oproportionerligt utnyttjande av resurser så som tid, kostnad och arbetskraft.

Samtycke innebär att den registrerade frivilligt och på ett entydigt sätt, genom ett utlåtande eller en åtgärd, indikerar att han eller hon vidkänner emottagande av information om, och uttryckligen går med på att dennes personuppgifter får behandlas enligt denna dataskyddspolicy . Samtycket måste dokumenteras på ett lämpligt sätt för att ha bevisvärde.

Personuppgiftsansvarig är den juridiska entitet inom koncernen som utifrån koncernens affärsverksamhet bestämmer hur och för vilka syften personuppgifter ska behandlas.

Konsekvensbedömning avseende dataskydd är en process som utförs och dokumenteras av den personuppgiftsansvarige, eller å dennes vägnar, om det krävs i tillämplig lagstiftning och efterfrågas av dataskyddsombudet. Detta ska ske innan nya teknologier för behandling, som skulle kunna hota en fysisk persons sekretesskydd, införs. Konsekvensbedömningen ska göras med hänsyn till vilken slags behandling som ska utföras, dess syften, omfattning och sammanhang. Bedömningen ska utföras för att analysera hur planerade behandlingsrutiner kommer att påverka personuppgiftsskyddet.

Den registrerade är en fysisk eller juridisk person (enligt tillämplig lagstiftning) vars personliga information berörs av behandlingen.

Dataskyddsombud är en person som utsetts av styrelsen för att informera och ha en rådgivande funktion inom koncernen angående tillämplig sekretesslagstiftning och denna policy. Det faller också inom ombudets ansvar att överse att tillämpliga regler efterföljs samt att fungera som kontaktperson för lokala tillsynsmyndigheter.

Lokala dataskyddssamordnare ska separat utses av den lokala ledningen, i samarbete med dataskyddsombudet, i varje koncernföretag. Rollen som dataskyddssamordnare kan även tilldelas den som är Compliance-agent i ett koncernföretag.

Personuppgifter omfattar all information som har samband med en identifierad eller identifierbar fysisk eller juridisk person (enligt tillämplig lagstiftning) (“den registrerade”). En person anses, direkt eller indirekt, vara identifierbar genom namn, identifikationsnummer, lokaliseringsuppgifter, nätidentifikationer eller andra (en eller flera) faktorer som specificerar en fysisk persons fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Personuppgiftsbiträde är en fysisk eller juridisk person, myndighet eller annan entitet som hanterar personuppgifter å den personuppgiftsansvariges vägnar.

Behandling av personuppgifter innefattar alla slags automatiserade och icke automatiserade processer genom vilka personuppgifter eller grupper av personlig information behandlas/hanteras inklusive insamling, registrering, organisering, strukturering, förvaring, anpassning, ändring, återvinning, användning eller tillgängliggörande genom överföring eller spridning (eller att informationen på annat sätt görs tillgänglig), kompilering och radering av personliga uppgifter. I detta sammanhang gäller dessa riktlinjer också för begreppen “behandlad” och ”behandlas”.

Pseudonymisering innebär behandling av personuppgifter på ett sådant sätt (t.ex. genom en lista där namn ersatts med nummer) att uppgifterna avidentifieras och inte längre kan kopplas samman med en viss registrerad utan användning av ytterligare information. Detta under

förutsättning att den kompletterande informationen, genom vilken identifiering kan ske, förvaras separat på ett sådant sätt som säkerställer att den inte kan kopplas samman med en identifierad eller identifierbar fysisk person.

Känsliga personuppgifter är sådana som identifierar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk tro, facklig tillhörighet, behandling av genetiska och biometriska uppgifter i syfte att identifiera en fysisk person och uppgifter angående en persons sexliv eller sexuell läggning. Beroende på tillämplig lagstiftning kan känsliga personuppgifter också inkludera information om sociala åtgärder såväl som administrativa eller straffrättsliga förfaranden och sanktioner.

Tredje part är en fysisk person eller juridisk entitet, en offentlig myndighet eller annan entitet som inte faller under den personuppgiftsansvariges ansvar och inte heller är en registrerad person eller ett personuppgiftsbiträde eller på annat sätt är direkt underordnad den personuppgiftsansvarige eller ett personuppgiftsbiträde, vilken har befogenhet att behandla personuppgifter. Detta innebär att alla företag inom koncernen såväl som alla utomstående affärspartners ska anses vara tredje parter, förutom om de behandlar uppgifter i egenskap av personuppgiftsbiträden för något annat företag inom gruppen (t.ex. genom att tillhandahålla stödtjänster inom informations- och kommunikationsteknologi).

Överföring innefattar allt slags tillgängliggörande genom vidarebefordring eller distribution av personuppgifter samt alla andra slags former av överflyttning från den personuppgiftsansvarige till tredje part.

5. Ansvar enligt denna policy

5.1 Dataskyddsombudet är ansvarig för uppsättande, ändring och kontroll av koncernens dataskyddspolicy. Dessutom är dataskyddsombudet ansvarig för policyns distribution inom koncernen.

5.2 Styrelsen är ansvarig för att koncernens dataskyddspolicy godkänns.

6. Principer gällande behandling av personuppgifter

Behandling av personuppgifter ska ske i enlighet med internationell och nationell lagstiftning angående sekretess och personuppgiftsskydd såväl som i enlighet med interna policys och riktlinjer.

Principerna innefattar de allmänna skyldigheter som den personuppgiftsansvarige och andra inblandade parter har för att försäkra skydd för personuppgifter på ett lagligt och rättvist sätt. Principerna ger riktlinjer för hur behandling av personuppgifter ska hanteras genom att tydliggöra under vilka förutsättningar detta ska ske:

6.1 Lagligt, rättvist och öppet

Personuppgifter ska behandlas på ett lagligt sätt, i god tro och på ett öppet sätt så att den registrerade har insyn i hur dennes uppgifter hanteras.

6.2 Ändamålsenligt

Koncernen ska endast samla in personuppgifter i befogade, specifika syften och har inte rätt att behandla dessa uppgifter i ytterligare syften som står i strid med de ursprungliga skälen för att samla in informationen, såvida det inte finns rättslig grund för att ändra syftena.

6.3 Dataminimering

Behandlingen av personuppgifter måste vara nödvändig för att uppfylla de avsedda syftena. Behandlingen ska vara relevant och tillräcklig för att uppfylla syftena men inte gå utöver vad som behövs för att uppfylla dem.

6.4 Riktighet
Alla personuppgifter måste vara faktiskt korrekta och om så behövs hållas uppdaterade. Eftersom felaktig behandling av personuppgifter på många olika sätt kan innebära risker för både de registrerade och företagen inom koncernen ska den personuppgiftsansvarige vidta lämpliga och rimliga åtgärder för att säkerställa att felaktig information utan dröjsmål antingen rättas eller raderas med hänsyn till de syften för vilka de behandlas.

6.5 Lagringsbegränsningar
Personuppgifter ska inte lagras på ett sådant sätt som medger identifiering av den registrerade längre än vad som behövs utifrån de syften för vilka de behandlas.

6.6 Säkerhet: sekretess, integritet och tillgänglighet
För att personuppgifterna ska kunna skyddas måste den personuppgiftsansvarige genom att vidta lämpliga tekniska och organisatoriska åtgärder se till att en lämplig nivå av säkerhet uppnås, inklusive skydd från obehörig och olaglig behandling samt skydd från oavsiktlig förlust, radering eller skada.

Beslut om vilka tekniska och organisatoriska åtgärder som ska anses vara lämpliga ska fattas med hänsyn till storleken och sannolikheten av eventuella hot och dess inverkan på de fysiska personernas rättigheter och friheter samt även utifrån kostnaden för att implementera åtgärderna utifrån arten, omfattningen, sammanhanget och syftet med behandlingen.

Dessa åtgärder kan inkludera:

- anonymisering, pseudonymisering och/eller kryptering av personuppgifter,
- att säkerställa att de hanteringssystem och tjänster som används kontinuerligt upprätthåller sekretess, integritet, tillgänglighet och motståndskraft,
- i det fall att ett fysiskt eller tekniskt avbrott uppstår, förmåga att inom rimlig tid kunna återställa tillgänglighet till personuppgifter, och
- rutiner för att regelbundet testa och utvärdera hur effektiva de tekniska och organisatoriska åtgärderna är för att säkerställa säker behandling.

Utöver dessa krav, ska all behandling av personuppgifter inom koncernen, eller å våra vägnar, ske i enlighet med de restriktioner och regler för tekniska och organisatoriska åtgärder som återfinns i våra riktlinjer för användning, säkerhet och kontroll av informationsteknologi.

6.7 Ansvarig
Den personuppgiftsansvarige ansvarar för att principerna i punkterna 6.1 till 6.5 följs och måste kunna visa att så skett. Denne måste därför löpande och för all behandling dokumentera hur principerna tillämpas för att kunna bevisa att de följs.

7. Särskilda åtgärder för att upprätthålla sekretess inom Ivoclar Vivadent koncernen

Det är förbjudet för anställda att använda företagsinformation eller personuppgifter för privat bruk, i personliga syften eller att på något sätt tillgängliggöra sådan information till obehöriga personer eller entiteteter.

I denna policy ska termen ‘obehörig’ förstås som hantering av personuppgifter av anställda som inte behöver tillgång till dessa för att kunna utföra sitt jobb enligt sina arbetsbeskrivningar. Olika anställdas roller och ansvarsområden vad gäller behandling av personuppgifter ska klargöras av den personuppgiftsansvarige på ett sådant sätt att det säkerställer att anställda endast har tillgång till den information som är lämplig och behövs för att de ska kunna utföra sina specifika uppgifter.

Endast behörig personal som har skyldighet att upprätthålla datasekretess ska tillåtas att behandla personuppgifter och endast för de avsedda syftena och inom existerande, säkra

informations- och kommunikationssystem. I enlighet med vad som gäller enligt tillämplig lokal lagstiftning betyder detta att ett separat dokument ska upprättas eller att det skrivs in ett villkor i ifrågavarande personals anställningskontrakt att de åtar sig att upprätthålla datasekretess även efter att ett anställningsförhållande upphört.

8. Behandling av känsliga personuppgifter

Utom i de fall det är absolut nödvändigt för att möta särskilda skyldigheter eller rättigheter och/eller den personuppgiftsansvarige har befogade skäl enligt tillämplig lagstiftning så ska känsliga personuppgifter endast behandlas efter den registrerades uttalade samtycke.

9. Lagliga grunder för behandling

9.1 Allmänna villkor för behandling av personuppgifter

Behandling av personuppgifter är endast laglig om åtminstone ett av de följande villkoren är uppfyllda:

- **Samtycke**: den registrerade har gett sitt uttryckliga samtycke till att personuppgifter behandlas i ett eller flera syften som de bestämts av den personuppgiftsansvarige,
- **Avtal**: behandling är nödvändig för att ett avtal ska kunna slutas mellan den registrerade och den personuppgiftsansvarige,
- i det fall att ett avtal redan slutits, behandling är nödvändig för utförandet av avtalet,
- **Rättslig förpliktelse**: behandling är nödvändig på grund av lagliga skyldigheter som den personuppgiftsansvarige har,
- **Skydda intresse av avgörande betydelse för den registrerades liv**: behandling är nödvändig för att skydda den registrerades eller annan fysisk persons vitala intressen,
- **Intresseavvägning**: den personuppgiftsansvarige eller tredje part har berättigat intresse och det inte finns tyngre vägande grundläggande rättigheter eller friheter på den registrerades sida som kräver personuppgiftsskydd,
- **Myndighetsutövning:** att det finns andra befogade skäl i enlighet med tillämplig lagstiftning.
- **Allmänt intresse:** På direkt uppdrag av riksdag, regering eller myndighet. Grundat på kommunala självstyret.

9.2 Särskilda villkor för videoövervakningssystem

Behandling av personlig information som kommer från videoövervakningssystem får endast ske med följande begränsningar.

Användning av videoövervakningssystem på allmänna platser och inom arbetsplatser är endast tillåten om:

- det finns befogade skäl utifrån den personuppgiftsansvariges intressen, t.ex. för anställdas och besökares säkerhet, åtkomstkontroll eller för att på annat sätt skydda den personuppgiftsansvariges egendom, anställda och besökare,
- användning begränsas i så hög utsträckning som möjligt (t.ex. vad gäller antal kameror, skärminspelning m.m.) utifrån de angivna syftena, och
- alla krav i tillämplig lagstiftning följs.

I det fall att det krävs enligt tillämplig lagstiftning ska nödvändiga tillstånd först sökas från behöriga myndigheter (dataskyddsmyndigheter, arbetsskyddsmyndigheter m.fl.).

Om de ovan angivna villkoren är uppfyllda och ett videoövervakningssystem installeras ska en separat policy för varje system upprättas i vilken det som ett minimum ska fastställas vilken teknologi som ska användas, vilket område som ska övervakas, vem som har tillgång till kamera och inspelningar, tidsbegränsningar för lagring, rutiner för radering samt rutiner för, och under vilka villkor inspelningar får lämnas över till tredje parter, särskilt offentliga myndigheter.

10. Behandling å personuppgiftsansvariges vägnar

I det fall den personuppgiftsansvarige anlitar ett personuppgiftsbiträde för att behandla personuppgifter å sina vägnar kvarstår ansvaret för att behandlingen sker i enlighet med tillämplig lagstiftning och andra regler på den personuppgiftsansvarige.

Av det skälet ska den personuppgiftsansvarige endast anlita personuppgiftsbiträden som i tillräcklig grad kan garantera att tillräckliga tekniska och organisatoriska åtgärder kommer att användas för att säkerställa att de registrerades rättigheter upprätthålls.

Personuppgiftsbiträdets tjänster ska endast utföras inom ramen för ett skrivet avtal vilket ska specificera uppdragets natur, varaktighet, slag och syfte med behandlingen samt vilka kategorier av personuppgifter som ska behandlas. Avtalet ska även specificera vilka tekniska och organisatoriska åtgärder som ska användas (se punkt 6.6) av personuppgiftsbiträdet och vilka respektive rättigheter och skyldigheter den personuppgiftsansvarige och personuppgiftsbiträdet har.

I det fall personuppgiftsbiträdet i sin tur behöver anlita ytterligare personuppgiftsbiträden får detta endast ske efter uttryckligt skriftligt medgivande från den personuppgiftsansvarige.

De lokala dataskyddssamordnarna ska kontaktas så snart som möjligt i processen för att etablera och upprätta ett avtal mellan den personuppgiftsansvarige och personuppgiftsbiträdet.

11. Överföring av personuppgifter till tredje part

Den personuppgiftsansvarige ska inte överföra några personuppgifter till tredje part om inte tillräckliga åtgärder har vidtagits för att sådan överföring kan ske säkert och lagligt i enlighet med tillämplig lagstiftning.

Varje gång den personuppgiftsansvarige överför personuppgifter till en tredjepartsleverantör som ska utföra en tjänst och behandla uppgifterna å den personuppgiftsansvariges vägnar är reglerna i punkt 10 tillämpliga.

I vissa situationer kan personuppgifter behöva överföras till myndigheter eller andra officiella organ i enlighet med tillämplig lagstiftning. Vid sådan förfrågan ska den personuppgiftsansvarige se till att dataskyddsombudet omedelbart informeras samt också i den utsträckning det är lagligt försöka vägra eller begränsa sådan överföring och i synnerhet se till att endast personuppgifter som är relevanta och nödvändiga enligt förfrågan lämnas ut.

I det fall personuppgifter överförs utomlands kan det ställas särskilda krav enligt det landets tillämpliga lagstiftning. Detta gäller särskilt, men inte endast, när personuppgifter överförs från länder inom den Europeiska Ekonomiska Samarbetsunionen (ESS) till länder utanför ESS. De lokala dataskyddsamordnarna bör kontaktas så snart som möjligt för att säkerställa att nationell tillämplig lagstiftning följs.

12. De registrerades rättigheter

Varje registrerad har i förhållande till den personuppgiftsansvarige absoluta och omfattande rättigheter i enlighet med tillämplig lagstiftning. Dessa rättigheter kan varken helt skrivas bort eller begränsas genom avtal eller andra rättsliga åtgärder.

12.1 Information till personuppgifter

Principen avseende öppenhet och insyn innebär att personuppgifter måste hanteras på ett öppet sätt med insyn för den registrerade. Den personuppgiftsansvarige ska ge den registrerade information i enlighet med de krav som ställs i tillämplig lagstiftning.

För ytterligare information vänligen kontakta dataskyddsombudet.

12.2 Rätt till tillgång
Varje registrerad har rätt att efterfråga information gällande personuppgifter lagrade inom koncernen. Den information som tillhandahålls ska som ett minimum innehålla uppgifter i enlighet med vad som krävs i tillämplig lagstiftning.

Den registrerade ska skicka en ansökan om att få ta del av information till ansvarig avdelning inom respektive Ivoclar Vivadent-entitet och de är skyldiga att hjälpa till i nödvändig utsträckning.

12.3 Rätt till rättelse
Om de lagrade personuppgifterna är felaktiga eller ofullständiga har den registrerade möjlighet att kräva rättelse av uppgifter som rör honom eller henne. Vidare har en registrerad möjlighet att kräva att personuppgifter kompletteras med hänsyn till syftet för vilket de behandlas.

12.4 Rätt till radering ("rätten att bli glömd")
Den registrerade har möjlighet att kräva att personuppgifter raderas och den personuppgiftsansvarige är skyldig att tillmötesgå detta krav om behandling inte längre är befogad eller nödvändig i enlighet med tillämplig lagstiftning.

Skäl för radering kan vara:

- att personuppgifterna inte längre är nödvändiga utifrån de syften för vilka de samlades in eller behandlades,
- den registrerade tar tillbaka sitt medgivande på vilket behandlingen är baserad och det inte finns något annat befogat skäl för behandling,
- den registrerade motsätter sig behandlingen i enlighet med punkt 12.7 och det inte finns några andra befogade skäl för behandlingen som väger tyngre,
- behandlingen av personuppgifter är olaglig, eller
- personuppgifter måste raderas för att tillmötesgå krav i tillämplig lagstiftning som den personuppgiftsansvarige faller under.

12.5 Rätt till begränsning av behandling
Den registrerade har möjlighet att begränsa behandling och den personuppgiftsansvarige är skyldig att tillmötesgå detta krav och begränsa behandlingen av personuppgifterna i den utsträckning detta följer av tillämplig lagstiftning.

12.6 Rätt till dataportabilitet
På begäran måste den personuppgiftsansvarige kunna tillhandahålla den registrerade dess personuppgifter i ett strukturerat, vanligen använt och maskinläsbart format så att den registrerade kan flytta över sina uppgifter till en annan personuppgiftsansvarig utan att detta förhindras av den personuppgiftsansvarige till vilken uppgifterna till en början uppgavs. Detta under förutsättning att en sådan rätt till portabilitet återfinns i tillämplig lagstiftning.

I det fall en registrerad vill utöva sin rätt att flytta över personuppgifter har denne rätt att få en överföring direkt från en personuppgiftsansvarig till en annan om detta är tekniskt möjligt.

12.7 Rätt att göra invändningar
I det fall behandlingen baseras på ett befogat intresse som den personuppgiftsansvarige eller en tredje part har och dessa intressen inte står i strid med den registrerades grundläggande rättigheter och friheter så har den registrerade fortfarande ändå rätt att komma med invändningar mot hur dennes personuppgifter behandlas i den utsträckning det tillåts i tillämplig lagstiftning.

12.8 Rätt till ersättning för skada

Beroende på tillämplig lagstiftning kan den registrerade ha möjlighet att kräva ersättning för skada som denne åsamkats till följd av felaktiga, ofullständiga, gamla, falska, olagligt insamlade eller genererade personuppgifter samt för obehörig behandling av personuppgifter.

12.9 Frågor, klagomål och avhjälpande åtgärder

Alla frågor, klagomål och beslut avseende avhjälpande åtgärder, inklusive skadeståndskrav, som har med dataskydd att göra ska uteslutande hanteras av dataskyddsombudet eller de lokala dataskyddssamordnarna som beskrivet i punkt 14.

13. Integrerad dataskyddshantering

13.1. Dataskyddsombud och tillsynsråd

Dataskyddsombudet tillsammans med Compliance Board är ansvariga för att denna policy och tillämplig lagstiftning följs. Inom detta ansvarsområde ligger att dataskyddsombudet, efter samråd med Compliance Board, etablerar och implementerar nödvändiga affärsdokument och rutiner för dataskydd och sedan övervakar att dessa följs.

Dataskyddsombudet ska utses utifrån professionella kvalifikationer. I synnerhet expertkunskap om dataskyddslagstiftning och hur dessa ska tillämpas samt förmåga att utföra de uppgifter som beskrivs nedan. Dataskyddsombudet ska vara bunden av sekretess när det gäller hur dennes arbetsuppgifter utförs. Vidare ska dataskyddsombudet finnas lättillgänglig för alla företag inom koncernen.

Dataskyddsombudet har följande arbetsuppgifter:

- Att informera och ge råd till den personuppgiftsansvarige och de anställda som hanterar personuppgifter angående deras skyldigheter för att skydda uppgifterna i enlighet med dataskyddslagstiftning och denna policy.
- Att övervaka att allmänna regler i denna policy och tillämplig dataskyddlagstiftning följs vilket inkluderar tilldelning av ansvar, utbildning av personal som behandlar personuppgifter, att det upprätthålls en allmän medvetenhet om dessa frågor och att hantera relaterade granskningar.
- Att på begäran ge råd angående nödvändiga konsekvensbedömningar gällande uppgiftsskydd och att övervaka dess utförande.
- Att samarbeta med tillsynsmyndigheter.
- Att agera som kontaktperson för nationella tillsynsmyndigheter angående frågor som har med behandling av personuppgifter att göra, inklusive vid förhandssamråd och att, i de fall det är lämpligt, också ge råd i andra frågor.

13.2 Lokala dataskyddssamordnare

De lokala dataskyddsamordnarna ska stödja dataskyddsombudet i utförandet av dennes arbetsuppgifter. För att dataskyddsombudet ska kunna fullgöra sina skyldigheter ska den lokala dataskyddssamordnaren fungera som dataskyddsombudets primära kontaktperson. De ger stöd genom att samla in nödvändig information och förmedlar denna till dataskyddsombudet. Vidare ska de också delge de lokala företagen inom koncernen nödvändig information om krav och standarder gällande dataskydd.

I samarbete med dataskyddsombudet ska de lokala samordnarnas arbetsuppgifter särskilt inkludera:

- att ge assistans, vägledning och information till den personuppgiftsansvarige och de registrerade,
- att erbjuda och genomföra lämpliga utbildningar, och
- att utföra konsekvensbedömningar av uppgiftsskydd å den personuppgiftsansvariges vägnar samt inför förhandssamråd och kontroller.

Compliance Board, kan komma att reglera dataskyddssamordnarnas arbetsuppgifter i en separat policy. I det fall en dataskyddsamordnare också är utsedd till dataskyddsombud ska

denna utöver samordnaransvar också utföra alla uppgifter som enligt tillämplig lagstiftning ska utföras av dataskyddsombudet.

13.3 Samarbete

För att personuppgifter ska kunna skyddas krävs en samlad insats och nära samarbete mellan dataskyddsombudet, de lokala dataskyddsamordnarna och andra inblandade parter så att en adekvat dataskyddsnivå kan uppnås för att säkerställa att behandling av personuppgifter sker i enlighet med de krav som ställs i internationell och nationell tillämplig lagstiftning avseende dataskydd.

Företagen inom koncernen och dess anställda ska stödja dataskyddsombudet och de lokala dataskyddssamordnarna i deras arbete att fullgöra sina uppgifter. Frågor angående dataskyddsombudet och de lokala dataskyddsamordnarna ska besvaras ärligt och utan onödigt dröjsmål. Dataskyddsombudet och de lokala dataskyddsamordnarna ska informeras i följande fall:

- vid utveckling och introduktion av nya system och processer som har betydelse för dataskydd,
- vid väsentliga förändringar av existerande system och processer som har betydelse för dataskydd,
- vid anlitande av nya utomstående tjänsteleverantörer som kan komma att få tillgång till personuppgifter,
- vid väsentliga förändringar i avtal med utomstående tjänsteleverantörer som kan komma att få tillgång till personuppgifter,
- vid förfrågningar från kunder, anställda, arbetskommittéer, samarbetspartners eller andra registrerade som kan ha betydelse för dataskydd, och
- vid förfrågningar från företag och/eller särskilda projekt om hjälp och råd avseende dataskydd.

Om det finns tecken på att kraven enligt tillämplig skyddslagstiftning eller denna policy inte efterlevs ska dataskyddsombudet, ledningen i ifrågavarande Ivoclar Vivadent-företag och tillsynsrådet informeras. Tillsynsrådet ska i samarbete med dataskyddsombudet klassificera incidenten och samordna vidare åtgärder. Om så krävs enligt lagstiftning ska tillsynsrådet också se till att berörda tillsynsmyndigheter och berörda registrerade blir informerade.

14. Frågor, klagomål och avhjälpande åtgärder

En registrerad har möjlighet att när som helst kontakta dataskyddsombudet eller en lokal dataskyddssamordnare och ställa frågor eller framföra klagomål avseende behandlingen av dennes personuppgifter. Samordnare ska i samtliga fall informera ombudet om sådana förfrågningar. Alla frågor och klagomål ska hanteras konfidentiellt.

I de fall en registrerad har frågor eller klagomål och anser att ett företag inom koncernen brutit mot reglerna i denna policy eller tillämplig lagstiftning och detta företag inte är beläget i samma land som den registrerade har denne möjlighet att välja om den vill kontakta företagets dataskyddssamordnare, en dataskyddssamordnare i det egna landet eller dataskyddsombudet direkt.

De förfaranden som beskrivs i denna policy gäller utöver andra rättsliga processer och rättsmedel.