# Koncernomfattande dataskyddspolicy för PHOENIX group

**GGL_Corporate Data Protection_20210201**

| | |
|---|---|
| Träder i kraft: | 2021-01-02 |
| Intern publicering | JA |
| Ersättningsriktlinje: | GGL_Group Data Protection_20171219 |

Täckning:

| | |
|---|---|
| Koncernomfattande | X |
| Undergrupp Tyskland | |
| PHOENIX | |

**Godkänd:** **2020-11-17**

## Koncernomfattande dataskyddspolicy för PHOENIX group

### Versionskontroll

| Version | Titel | Skribent | Datum |
|---|---|---|---|
| 01 EN | Koncernomfattande dataskyddspolicy för PHOENIX group | Barbora Seigertschmid | 2020-11-17 |
| | | | |
| | | | |
| | | | |

| Version | Villkor som berörs av revidering | Skribent | Datum |
|---|---|---|---|
| 01 EN | första versionen | Barbora Seigertschmid | 2020-11-17 |
| | | | |
| | | | |
| | | | |

### Signaturer/godkännanden

| Namn, avdelning | Roll | Datum |
|---|---|---|
| **Barbora Seigertschmid**<br>**HCDP** | Författare | **2020-11-17** |
| **Sven Seidel**<br>**CEO** | Godkännande | **2020-11-17** |
| **Helmut Fischer**<br>**CFO** | Godkännande | **2020-11-17** |

## Företagsdataskydd – ordlista

| | |
|---|---|
| CIO | Informationschef (Chief Information Officer) |
| CISO | Informationssäkerhetschef (Chief Information Security Officer) |
| CDP-guide | Guide för skydd av företagsdata |
| Företagskoncept | Koncept för skydd av företagsdata |
| Dataskyddspolicy | Koncernomfattande dataskyddspolicy för PHOENIX group |
| DPA | Databehandlingsavtal |
| DPIA | Konsekvensbedömning avseende dataskydd |
| DPO | Dataskyddsombud |
| Medarbetare | En person som är anställd av PHOENIX group. |
| EU/EES | Europeiska unionen/Europeiska ekonomiska samarbetsområdet |
| GDPR | Dataskyddsförordningen (EU) 2016/679 (GDPR). |
| HCDP | Dataskyddsansvarig (Head of Corporate Data Protection) |
| LSC | Lokal säkerhetskoordinator |
| Lokalt koncept | Lokalt dataskyddskoncept |
| PIA | Konsekvensbedömning avseende sekretess |
| PHOENIX-företag | Dotterbolag som tillhör PHOENIX group |
| PHOENIX group | Omfattar alla bolag i vilka en majoritet av aktierna innehas av PHOENIX Pharma SE eller något av dess dotterbolag, eller som direkt eller indirekt kontrolleras av holdingbolaget eller dess dotterbolag |
| SA | Tillsynsmyndighet |
| SOP | Operativa standardförfaranden |
| TOM | Tekniska och organisatoriska åtgärder |

## 1. Inledning

(1) Vi lever i en datadriven värld. Våra kunder, medarbetare och affärspartner delar sina data med oss i nästan varje transaktion och interaktion. Personuppgifter är information som gör att en levande person direkt, eller indirekt, kan identifieras utifrån tillgängliga data. Det kan vara uppgifter som en persons namn, platsdata, hälsodata eller något mindre uppenbart som IP-adresser.

(2) Personuppgifterna tillhör en levande person (**den registrerade**). Dataskydd ser till att allas personuppgifter används korrekt och lagenligt. Dataskyddslagar fastställer huvudprinciperna och reglerna för personuppgiftsbehandlingen.

(3) PHOENIX group tar dataskydd och sekretess för sina medarbetares, affärspartners och kunders data på stort allvar. Denna Dataskyddspolicy syftar till att säkerställa att personuppgiftsbehandlingen följer dataskyddslagstiftningen och återspeglar därför skyldigheter och principer i Dataskyddsförordningen.

## 2. Omfattning

(1) Denna policy ska tillämpas på behandling av personuppgifter som avser fysiska personer som kan identifieras utifrån dessa uppgifter. Den ska tillämpas på uppgifter som behandlas antingen elektroniskt eller som är pappersbaserade och som lagras i ett relevant register. I länder där uppgifter om juridiska personer (t.ex. aktiebolag) skyddas i samma utsträckning som personuppgifter, gäller denna policy i samma omfattning uppgifter om juridiska personer.

(2) Denna policy gäller:

a) alla medarbetare i PHOENIX group.
b) alla PHOENIX-företag.
c) enheter med vilka ett kontrakt har undertecknats med uppgifter om att denna policy måste tillämpas för tillgång till koncernens informationsresurser (joint venture-partner, franchisepartner osv.).
d) varje tredje part som direkt får tillgång till de informationstillgångar som ägs av eller är under direkt kontroll av PHOENIX group (t.ex. externa konsulter).
e) alla tjänstleverantörer som direkt får tillgång till de informationstillgångar som ägs av eller är under direkt kontroll av PHOENIX group. Dessa måste visa att denna policy efterlevs.

(3) Alla externa tjänstleverantörer och entreprenörer, som direkt får tillgång till de informationstillgångar som ägs av eller står under direkt kontroll av PHOENIX group måste enligt avtal vara skyldiga att följa denna policy och omfattas av sekretess. Varje tjänstleverantör som betraktas som personuppgiftsbiträde måste underteckna avtal om databehandling (se kapitel 6).

(4) PHOENIX-företaget ska utöva sin auktoritet över sina medarbetare och tillämpa denna policy i de lokala bindande reglerna för medarbetare, enligt den lokala arbetsrätten.

(5) PHOENIX-företaget ska se till att alla dess medarbetare vid behov har lämplig tillgång till denna policy på sitt lokala språk, framför allt via intranätet. Den ursprungliga engelska versionen har företräde.

(6) Denna policy är en av de implementeringsåtgärder som krävs för att uppnå efterlevnad av Dataskyddsförordningen. Ytterligare implementeringsåtgärder beskrivs i kapitel 10.

(7) Nationell lag och nationella förordningar kan vara strängare än Dataskyddsförordningen och/eller denna policy. Alla PHOENIX-företag och deras medarbetare ska följa tillämpliga lokala lagar.

(8) Lokal anpassning får göras, men får inte medföra att dataskyddsnivån sjunker under det som beskrivs i denna policy. Avvikelser från denna policy eller från företagets dataskydds-regler får endast beviljas genom undantag av PHOENIX group (dataskyddsansvarig, koncernledningen för PHOENIX group). Begäran om och godkännande av undantag ska dokumenteras. En mall för begäran om undantag kan erhållas från dataskyddsansvarig.

## 3. Organisation: Roller och ansvar med avseende på dataskydd

### 3.1 Koncernledning (koncernnivå)

(1) Dataskyddsansvarig (HCDP) stödjer PHOENIX groups koncernledning i arbetet med att organisera, genomföra, underhålla, granska och förbättra företagsdataskyddet. Koncernledningen begär definierade rapporter från dataskyddsansvarig.

(2) För att dataskyddsansvarig ska kunna fullgöra sina uppgifter ska koncernledningen automatiskt informera och, om det är tillämpligt, involvera dataskyddsansvarig på lämpligt sätt och i god tid om/i alla internationella frågor, projekt, förändringar eller operationer som är kopplade till personuppgiftsbehandling (passiv rätt till information). Koncernledningen ska stödja dataskyddsansvarig i utförandet av hans/hennes uppgifter.

(3) Dataskyddsansvarig ska ha tillgång till resurser som speglar affärsmodellens karaktär och komplexitet inom koncernen. Dataskyddsansvarig har en oberoende ställning i organisationen och rapporterar till medlemmarna i koncernledningen.

### 3.2 Styrelse (företagsnivå)

(1) PHOENIX-företaget ska utvärdera om utnämning av ett dataskyddsombud (DPO) är obligatoriskt enligt lokal lag och uppfylla ytterligare rättsliga krav som är relaterade härtill (t.ex. informera datainspektionen, offentliggöra kontaktuppgifter till det lokala dataskyddsombudet osv.).

(2) Om det inte finns någon rättslig skyldighet att utse ett dataskyddsombud enligt Dataskyddsförordningen eller den lokala dataskyddslagen, ska PHOENIX-företaget utse en kontaktperson för dataskyddsuppgifter och kommunikationen med företagsdataskydd. I intern kommunikation kallas personen dataskyddsombud. Denna förkortning innebär inte att personen är ett officiellt utsett dataskyddsombud i enlighet med Dataskyddsförordningen.

(3) Alla externa tjänstleverantörer som agerar som dataskyddsombud för PHOENIX-företaget måste enligt avtal vara skyldiga att följa denna policy.

(4) PHOENIX-företag från ett land kan besluta att en person ska företräda dem i kommunikationen med företagsdataskyddet.

(5) Officiellt eller internt utsett dataskyddsombud ska ha erforderliga yrkesmässiga kvalifikationer och kunskaper om lagstiftning och praxis avseende dataskydd.

(6) För att dataskyddsombudet ska kunna fullgöra sina uppgifter ska den lokala styrelsen automatiskt informera och, om det är tillämpligt, involvera dataskyddsombudet på lämpligt sätt och i rätt tid om/i alla internationella frågor, projekt, förändringar eller

operationer som är kopplade till reglerna för skydd av personuppgifter. Den lokala styrelsen ska stödja dataskyddsombudet i utförandet av hans/hennes uppgifter.

(7) Dataskyddsombudet ska ha tillgång till resurser som speglar affärsmodellens karaktär och komplexitet inom PHOENIX-företaget. Dataskyddsombudet har en oberoende ställning i PHOENIX-företaget och rapporterar till högsta ledningsnivå.

(8) Styrelsen, oavsett om den utför processens roll eller inte, är ansvarig för dataskydd. Styrelsen ska se till att dataskyddslagstiftningen och denna policy följs genom att exempelvis utforma lämpliga organisationsstrukturer och procedurer, så att verksamhetsstyrningen får resurser och bemyndigande att effektivt utföra rollen som processägare och säkerställa efterlevnad.

(9) Alla medarbetare ska ha korrekt tillgång till befintliga riktlinjer och rutiner för dataskydd som motsvarar befattningen. Policyer, förfaranden samt ansvar och funktioner avseende dataskydd ska övervakas och underhållas regelbundet (vartannat år). Dataskyddsombudet ansvarar för denna lokala övervakning.

### 3.3 Medarbetare

(1) Alla medarbetare förväntas upprätthålla sekretess när det gäller personuppgifter som behandlas av PHOENIX-företaget. Denna skyldighet skall införlivas i anställningsavtalet och/eller i dokumentationen för nyanställda.

(2) Adekvat utbildning i dataskydd (online och/eller personligen) är obligatorisk för alla medarbetare i PHOENIX group med avseende på arbetsuppgift och ansvar. Utbildningsplanen tillhör implementeringsåtgärderna (se kapitel 10).

(3) Alla medarbetare stödjer dataskyddsombud och dataskyddsansvarig i fullgörandet av dennes arbetsuppgifter, till exempel genom att ge dem tillgång till personuppgifterna (vid begäran från registrerad) och genom att utföra begärda uppgifter, tillhandahålla information eller lämna över handlingar.

(4) Alla medarbetare involverar dataskyddsombud/dataskyddsansvarig i ett tidigt skede i alla frågor som rör skydd av personuppgifter.

(5) Alla medarbetare iakttar och följer dataskyddsprinciperna vid behandling av data (se kapitel 4).

(6) Alla medarbetare rapporterar dataintrång internt (se kapitel 9).

### 3.4 Processägare

(1) Den medarbetare i PHOENIX-företaget som är begreppsmässigt ansvarig för ett affärsförfarande eller en intern process där personuppgifter behandlas anses vara processägare.

(2) Processägaren ansvarar för den så kallade behandlingsåtgärden. Behandlingsåtgärd är en uppsättning operationer, till exempel en specifik affärsprocess eller ett IT-verktyg.

(3) Processägaren namnges i uppgifterna om behandlingsåtgärder per namn eller funktion (se kapitel 5).

(4) Vid planering, införande och senare ändring av behandlingsåtgärden ska processägaren följa dessa regler:

a) Involvera dataskyddsombudet i en (för)bedömning av sekretesspåverkan.

b) Utföra en konsekvensbedömning avseende dataskydd, om en sådan är obligatorisk (se kapitel 5).
c) Skapa och underhålla dokumentationen om behandlingsåtgärder (se kapitel 5).
d) Tillse informationen för de registrerade om databehandlingen.
e) Säkerställa att principerna för dataskydd iakttas under behandlingen (genom att involvera berörda avdelningar).
f) Granska den externa tjänstleverantören. Om tjänsteleverantörer behandlar uppgifter för PHOENIX-företaget på uppdrag av och i enlighet med företagets instruktioner, säkerställa att avtalen om databehandling ingås.
g) Säkerställa att de registrerades rättigheter kan uppfyllas.
h) Säkerställa att åtkomsträttigheter och lagringsperioder definieras i samband med implementering.
i) Vid överföring av data till länder utanför EU/EES, involvera dataskyddsombudet och iaktta de särskilda kraven för databehandling utanför EU/EES.
j) Dokumentera allt på ett sådant sätt att det går att bevisa att bestämmelserna om uppgiftsskydd efterlevs.

(5) Det tekniska underhållet av behandlingsåtgärder kan överlåtas till en extern leverantör (se kapitel 6) eller IT-avdelningen, men processägaren ansvarar fortfarande för uppfyllandet av de regler som anges ovan. Dataskyddsombudet bistår och ger råd till processägaren.

(6) PHOENIX-företaget kan definiera en egen lämplig organisation för att hantera dataskydd och dess terminologi, roller och ansvar i enlighet med detta. Processägarens roll ska omfattas av den definierade organisationen.

## 3.5 Dataskyddsombud

(1) Dataskyddsombudets huvudsakliga uppgift är att skydda sekretessen för registrerade i förhållande till behandling av personuppgifter på företags-/landsnivå (uppgifter om kunder, patienter, anställda osv.). Dataskyddsombudet är den officiella kontakten för de registrerade och för tillsynsmyndigheten.

(2) Dataskyddsombudet ansvarar för rådgivning till organisation och medarbetare avseende dataskyddet. Dataskyddsombudet ansvarar för att bevaka att dataskyddslagen följs. Dataskyddsombudet definierar innehållet i det lokala konceptet (mer information finns i kapitel 10).

(3) Dataskyddsombudets huvudsakliga ansvarsområden är följande:
- Öka medvetenheten: kampanjer och utbildningsprogram.
- Underhålla den lokala dataskyddspolicyn och relaterade policyer eller instruktioner.
- Underhålla de nationella mallarna (databehandlingsavtal, sekretessmeddelande, samtycke osv.).
- Utgöra ett stöd vid förhandlingar om ett databehandlingsavtal (DPA): Översyn av större databehandlingsavtal och EU-standardklausuler. Dataskyddsombudet utgör ett stöd för den juridiska avdelningen och/eller inköpsavdelningen.
- Inledande bedömning av nya lokala projekt: definition av krav och rekommendationer för dataskydd.
- Bistå vid utförande av konsekvensbedömningar avseende dataskydd.
- Bistå vid skapande och underhåll av dokumentation av behandlingsåtgärder.

- Samordning av utövandet av den registrerades rättigheter: Upprätthållande av de interna processerna för utövande av den registrerades rättigheter.
- Stöd vid hantering av personuppgiftsincidenter och hantering av person-uppgiftsintrång: Samordning och hjälp vid rapportering till tillsynsmyndighet/de registrerade.
- Styrning och rådgivning: Löpande övervakning av efterlevnaden av dataskyddet

(4) Dataskyddsombudet informerar dataskyddsansvarig om dataskyddsfrågor eller större projekt med koppling till dataskyddet i PHOENIX-företaget. Dataskyddsombudet rapporterar till dataskyddsansvarig i de s.k. landsrapporterna årligen eller på begäran.

### 3.6 Företagsdataskydd

(1) Den huvudsakliga uppgiften för avdelningen för företagsdataskydd är att stödja PHOENIX group och dataskyddsombudet i dataskyddsarbetet.

(2) Dataskyddsansvarig har samma uppgifter som dataskyddsombudet men i ett internationellt sammanhang. Dataskyddsansvarig ger råd till och övervakar efterlevnaden av dataskyddslagarna inom koncernen. Dataskyddsansvarig samordnar och stödjer det internationella samarbetet gällande dataskyddet.

(3) Dataskyddsansvarig definierar innehållet i det företagskonceptet (mer information finns i kapitel 10).

(4) Dataskyddsansvarigs huvudsakliga ansvarsområden är följande:

- Öka medvetenheten: kampanjer och utbildningsprogram (inkl. onlineutbildning inom PHOENIX group).
- Underhålla den koncernomfattande dataskyddspolicyn.
- Skapa standarder för företagsdataskydd.
- Utgöra ett stöd vid förhandlingar om ett internationellt stort databehandlingsavtal (DPA):
- Inledande bedömning av nya lokala/internationella projekt: definition av krav och rekommendationer för dataskydd.
- Bistå i utförandet av konsekvensbedömningar avseende dataskydd på koncernnivå (företagsmallar för lokala dataskyddsombud).
- Underhålla koncernens rapporteringssystem för dataintrång: Administratör för rapporteringsplattformen.
- Underhålla av hanteringen vid dataintrång: Samordna och bistå vid rapportering till tillsynsmyndighet/de registrerade om internationella aspekter föreligger.
- Rådgivning och löpande övervakning av efterlevnaden av dataskyddet.

(5) Medlemmarna i företagsdataskyddet stödjer dataskyddsansvarigs arbete inom specifika områden lokalt eller internationellt. Medlemmar i företagsdataskyddet ska följa dataskyddsansvarigs anvisningar och rapporterar direkt till dataskyddsansvarig.

### 3.7 Informationssäkerhet

(1) Informationssäkerhetschefen (**CISO**) ansvarar för att säkerställa och genomföra informationssäkerhetsstandarderna i PHOENIX group. Informationssäkerhetschefen fastställer lämpliga säkerhetspolicyer, riktlinjer och standarder och definierar innehållet i säkerhetskonceptet för PHOENIX group.

(2) Informationssäkerhetschefen och den lokala säkerhetskoordinatorn (**LSC**) ansvarar för implementering och dokumentation av de tekniska och organisatoriska åtgärder (**TOM**) för att skydda personuppgifterna. Dokumentationen av TOM användas för att påvisa att säkerhetsprincipen i Dataskyddsförordningen följs (se kapitel 4).

(3) Det ska finnas ett nära samarbete och tät kommunikation mellan informationssäkerhetschefen och dataskyddsansvarig samt lokal säkerhetskoordinator och dataskyddsombud på lokal nivå med avseende på TOM. Dataskyddsansvarig/dataskyddsombud ska lista huvudkraven för TOM.

(4) Den lokala säkerhetskoordinatorn stödjer dataskyddsombudet vid granskningen av tjänstleverantörer. Den lokala säkerhetskoordinatorn kontrollerar TOM för den tjänsteleverantör som betraktas som personuppgiftsbiträde (se kapitel 6).

## 4. Rättslig ram för behandling av personuppgifter

(1) Listan nedan ger en översikt över allmänt erkända principer för dataskydd enligt den modell som återfinns i artikel 5 i Dataskyddsförordningen.

(2) Alla medarbetare är skyldiga att iaktta och följa dataskyddsprinciperna vid behandling av personuppgifter. Alla medarbetare ska följa dataskyddskraven i enlighet med sin funktion och roll i PHOENIX group och/eller i PHOENIX-företaget.

### Princip 1: Laglighet, korrekthet och öppenhet

(1) Behandlingen av personuppgifter måste vara rättvis, dvs. ingen oväntad eller vilseledande databehandling får utföras. Den registrerade måste få information om detaljerna rörande behandlingen av hans eller hennes personuppgifter.

(2) Personuppgifter får endast behandlas om det finns en rättslig grund för databehandlingen. Det finns sex rättsliga grunder för behandling:

**(a) Samtycke:** den enskilde har gett ett tydligt samtycke till behandling av sina personuppgifter för ett specifikt syfte.

**(b) Kontrakt:** behandlingen är nödvändig för ett kontrakt som PHOENIX-företaget har med individen eller för att specifika steg krävs innan ett kontrakt undertecknas.

**c) Rättslig skyldighet**: behandlingen är nödvändig för att följa lagen (ej inklusive avtalsförpliktelser).

**(d) Vitala intressen**: behandlingen är nödvändig för att skydda någons liv.

**(e) Offentlig uppgift**: behandlingen är nödvändig för att utföra en uppgift i allmänhetens intresse eller för en officiell funktion och uppgiften eller funktionen har en klar rättslig grund.

**(f) Legitima intressen:** behandlingen är nödvändig för PHOENIX-företagets legitima intressen eller tredje parts legitima intressen, såvida det inte finns goda skäl att skydda individens personuppgifter, vilket åsidosätter dessa legitima intressen.

(3) Om samma syfte kan uppnås utan personuppgiftsbehandlingen existerar ingen rättslig grund. Den rättsliga grunden måste definieras innan behandlingen påbörjas och måste dokumenteras i Register över behandlingsåtgärder (se kapitel 5).

(4) Ingen enskild grund är viktigare än de andra – vilken grund som är lämpligast att använda beror på syftet/syftena och förhållandet till den registrerade.

### Särskilda regler för samtycke

(1) Samtycke är inte i sig bättre eller viktigare än dessa alternativ. Samtycke innebär att erbjuda individer verkliga val och kontroll.

(2) Samtycke måste ges frivilligt. Samtycke ska vara uppenbart och kräver en positiv aktivitet för att välja att delta. Det finns ingen fastställd tidsgräns för samtycke och hur länge samtycket gäller beror på sammanhanget för databehandlingen.

### Särskilda regler om känsliga personuppgifter enligt Dataskyddsförordningen (GDPR)

(1) I Dataskyddsförordningen definieras känsliga personuppgifter som:
- personuppgifter som avslöjar ras eller etniskt ursprung,
- personuppgifter som avslöjar politiska åsikter,
- personuppgifter som avslöjar religiös eller filosofisk övertygelse;
- personuppgifter som avslöjar medlemskap i fackförening,
- genetiska data,
- biometriska data (där de används i identifieringssyfte),
- data som rör hälsa,
- data som rör en persons sexliv,
- data som rör en persons sexuella läggning.

(2) Vid behandling av känsliga personuppgifter gäller strängare regler. Utöver den rättsliga grunden måste ett av de särskilda villkoren i artikel 9 av Dataskyddsförordningen uppfyllas:
(a) Uttryckligt samtycke
(b) Sysselsättning, social trygghet och socialt skydd (om det är tillåtet enligt lag)
(c) Vitala intressen
(d) Icke-vinstdrivande organ
(e) Offentliggjort av den registrerade
(f) Rättsliga anspråk eller rättsliga handlingar
(g) Väsentligt allmänintresse (med rättslig grund)
(h) Vård eller omsorg (med rättslig grund)
(i) Folkhälsa (med rättslig grund)
(j) Arkivering, forskning och statistik (med rättslig grund)

(3) Dataskyddsombudet måste vara delaktigt i samtliga planeringar eller projekt som är kopplade till behandling av känsliga personuppgifter.

| Dataskyddskrav som rör laglighet, korrekthet och öppenhet |
|---|
| - Fastställ en tydlig rättslig grund innan behandlingsåtgärden påbörjas.<br>- Se till att behandlingsåtgärden inte överskrider gränserna för denna rättsliga grund.<br>- Utvärdera den rättsliga grunden med dataskyddsombudet och dokumentera den enligt lokala regler.<br>- Involvera dataskyddsombudet, om känsliga personuppgifter ingår i omfattningen.<br>- Säkerställ att processer, syfte och den rättsliga grunden är fullständigt dokumenterade.<br>- Informera de registrerade om behandlingen, t.ex. dess syfte och personuppgifts-ansvarigs identitet, kommunicera tydligt till registrerade hur, i vilken utsträckning och för vilka syften deras personuppgifter kommer att behandlas. |

- Respektera individers rätt att få tillgång till och korrigera sina uppgifter.
- Utveckla procedurer och instruktioner som tydligt förklarar hur de registrerade kan utöva sina rättigheter till åtkomst och att korrigera sina uppgifter i varje fas av databehandlingen.
- Implementera funktioner i systemet för att svara på åtkomst-, ändrings- eller blockeringsbegäranden och mot invändningar mot behandling.
- Använd interna regler för att granska den rättsliga grundens giltighet vid en ändring, t.ex. återtagande av samtycke.

**Krav på samtycke**

- Samtycket måste specifikt täcka den personuppgiftsansvariges namn (PHOENIX-företaget), syftena med behandlingen och typerna av behandlingsåtgärder.
- Uttryckligt samtycke måste bekräftas i ord och inte av någon annan positiv åtgärd. Vagt eller generellt samtycke är inte tillräckligt.
- Samtycke kräver en positiv handling för att delta. Använd inte förkryssade rutor eller någon annan metod för standardsamtycke.
- Håll samtyckesbegäranden åtskilda från andra villkor (samtyckesbegäranden måste vara tydliga, separata från andra villkor, koncisa, lätta att förstå samt användarvänliga).
- Undvik att göra samtycke till behandling en förutsättning för en tjänst.
- Gör det lätt att återta samtycke och berätta hur det går till.
- Spara bevis på samtycke – vem, när, hur, och vad du har uppgett.

## Princip 2: Syftesbegränsning

(1) Personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade syften och inte senare behandlas på ett sätt som är oförenligt med dessa syften.

(2) Om det nya syftet är förenligt behövs ingen ny rättslig grund för den fortsatta behandlingen.

(3) Om det nya syftet skiljer sig kraftigt från det ursprungliga syftet, är oväntat eller har en omotiverad inverkan på individen, är det sannolikt oförenligt med ditt ursprungliga syfte.

**Dataskyddskrav som är relaterade till syftesbegränsning**

- Behandla personuppgifter endast för angivna uttryckliga, legitima och begränsade syften.
- Begränsa behandlingen av uppgifter i ett IT-system till det huvudsakliga specificerade syftet.
- Säkerställ syftesbegränsning om olika slags uppgifter samlas in och behandlas för olika syften.
- Tillämpa interna regler för bedömning av kompatibilitetsbehoven från fall till fall för att möjliggöra en ändring av syftet.
- Ange syftet eller syftena för behandling av personuppgifter i den dokumentation som är obligatorisk för behandlingen (dokumentation) enligt artikel 30 av Dataskydds-förordningen.
- Informera registrerade på ett tydligt sätt om varje ändring av huvudsyftet med behandlingen av personuppgifterna.

### Princip 3: Uppgiftsminimering

(1) Personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de syften för vilka de behandlas.

(2) Personuppgifterna ska raderas om de inte längre behövs.

| Dataskyddskrav som är relaterade till uppgiftsminimering |
|---|
| - Identifiera den minsta mängd personuppgifter som behövs för att uppfylla syftet. Lagra denna information, men inte mer.<br>- Kontrollera regelbundet att personuppgifterna fortfarande är relevanta och adekvata för syftena och radera allt som inte längre behövs.<br>- Överväg om det är möjligt att använda särskild teknik för att öka sekretessen så att det blir möjligt att undvika överdriven användning av personuppgifter eller användning av anonymiserade uppgifter.<br>- Säkerställ att personuppgifterna är adekvata, relevanta och inte överdrivna för syftet. |

### Princip 4: Korrekthet

(1) Personuppgifter ska vara korrekta och om nödvändigt uppdaterade.

(2) Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.

| Dataskyddskrav som är relaterade till korrekthet |
|---|
| - Säkerställ att personuppgifter är korrekta och uppdaterade.<br>- Tillämpa processer för att säkerställa och upprätthålla korrektheten i behandlad data, t.ex. genom att automatiskt kontrollera kvaliteten på information som anges i systemet före behandling.<br>- Säkerställ att den registrerade har möjlighet att korrigera uppgifter som inte längre är korrekta. |

### Princip 5: Lagringsminimering

(1) Personuppgifter får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.

(2) Processägaren fastställer lagrings-/raderingsperiod och registrerar detta i FENIX-företagets lagringspolicy.

(3) Varje PHOENIX-företag har en lagrings-/raderingspolicy

| Dataskyddskrav som är relaterade till lagringsbegränsning |
|---|
| - Lagra inte personuppgifter längre än vad som krävs för det ursprungligen angivna syftet.<br>- Fastställ i förväg lagringstiden för uppgifter som lagras i en form som möjliggör identifiering av registrerade.<br>- Säkerställ att erforderliga lagringsperioder står i proportion till syftena med insamling av uppgifter och att de är tidsbegränsade. |

- Tilldela och hantera separat lagringstid som är relaterad till uppgifter som samlats in för andra syften.
- Särskild försiktighet måste iakttas om personuppgifter lagras på papper eftersom de är svårare att spåra.
- Utforma systemfunktioner för hantering av lagringstid och utför nödvändiga efterföljande åtgärder: radering eller anonymisering.

## Princip 6: Säkerhet (Integritet och konfidentialitet)

(1) PHOENIX-företaget ska vidta lämpliga tekniska och organisatoriska åtgärder (TOM) för att skydda personuppgifter på ett sätt som står i proportion till de föreliggande sekretessriskerna.

Sekretessrisk för en registrerad kan uppstå särskilt i följande fall:
- oplanerad destruktion av personuppgifter och/eller
- förlust av personuppgifter och/eller
- oplanerad modifiering av personuppgifter och/eller
- obehörigt röjande av personuppgifter och/eller
- obehörig åtkomst till personuppgifter.

(2) Vid bedömning av lämpliga TOM ska följande beaktas:
- teknik,
- kostnader för implementering,
- typ, omfattning, sammanhang och syften med behandlingen samt
- risken för varierande sannolikhet och allvarlighetsgrad för de registrerades rättigheter och friheter (dvs. sekretessrisk för kunder eller anställda osv.).

(3) TOM måste säkerställa konfidentialitet, sekretess och tillgänglighet i PHOENIX system och tjänster samt för de personuppgifter som behandlas inom dem.

**Dataskyddskrav som är kopplade till säkerhet (integritet och sekretess)**

- Följ policyer, riktlinjer, standarder eller informationsmaterial om informationssäkerhet.
- Involvera lokal säkerhetskoordinator eller informationssäkerhetschefen i behandlingsåtgärden om det är obligatoriskt enligt den koncernomfattande eller lokala policyn.
- Beakta sådant som riskbedömning, organisationspolicyer eller tekniska åtgärder vid planeringen av behandlingsåtgärden.
- Baserat på riskbedömningen ska organisatoriska och tekniska åtgärder utformas och genomföras för att begränsa riskerna till en acceptabel nivå.
- Undvik behandlingsåtgärder för vilka en begränsning inte är effektiv.
- Säkerställ att ett tydligt beslut fattas av den ansvariga ledning om vilka risker som är godtagbara och varför.
- Använd om det är lämpligt åtgärder som pseudonymisering och kryptering.

| Krav som rör informationssäkerheten |
|---|
| **Sekretess:**<br>Personuppgifter måste skyddas mot obehörigt eller oavsiktlig röjande. Både externa och interna angripare (t.ex. hackare, frustrerade eller nyfikna medarbetare) samt försumliga eller strukturella hot (t.ex. otränade medarbetare, rollbaserade tillståndskoncept) måste beaktas.<br><br>**Integritet:**<br>Personuppgifter måste tillhandahållas i sin helhet och korrekt. Obehöriga ändringar av uppgifterna måste identifieras (t.ex. genom loggning/loggfiler) och rutiner för korrigering måste finnas.<br><br>**Tillgänglighet:**<br>Personuppgifter måste finnas tillgängliga när det behövs. Detta kräver också att de kan återställas vid förlust eller förstörelse (t.ex. säkerhetskopior).<br><br>Ett förfarande för att regelbundet granska, bedöma och utvärdera TOM-effektiviteten måste finnas (t.ex. penetrationstest, extern och intern granskning). |

**Princip 7: Ansvarsskyldighet**

(1) PHOENIX-företaget ska ansvara för och kunna visa att principerna från Dataskydds-förordningen som anges ovan efterlevs.

(2) Bevis är nyckeluppgiften för alla relevanta medarbetare. När rutiner för ansvars-skyldighet tillämpas skapas dokumentation. Denna dokumentation kan användas som bevis på ansvarsskyldighet, ägarskap och efterlevnad av Dataskyddsförordningen.

(3) PHOENIX-företaget ska föra ett fullständigt register över behandlingsåtgärder. Alla medarbetare, framför allt processägare, är skyldiga att informera dataskyddsombudet i förväg (innan planer genomförs) om nya eller förändrade behandlingsåtgärder (se kapitel 5).

| Dataskyddskrav som är relaterade till ansvarsskyldighet |
|---|
| - Säkerställ att efterlevnad av ovanstående principer kan bevisas i lämplig dokumentation.<br>- Informera dataskyddsombudet om nya eller förändrade behandlingsåtgärder i förväg. Detta ska göras i tillräckligt god tid för att han/hon ska hinna utvärdera behandlingsåtgärden. |

# 5. Ny eller ändrad databehandlingsåtgärd

## 5.1 Standardmetod

(1) Dataskyddsombudet ska involveras i varje ny behandlingsåtgärd i förväg. Processägaren eller projektledaren ansvarar för relevant samråd med dataskyddsombudet.

(2) Dataskyddsombudet granskar den rättsliga grunden för databehandlingen. Data-skyddsombudet listar de huvudsakliga dataskyddskraven i konsekvensbedömningen avseende sekretess (**PIA**). Omfattningen av konsekvensbedömningen avseende sekretess

beror på behandlingsåtgärden. Dataskyddsombudet anger om en konsekvensbedömning avseende dataskydd (DPIA) är obligatorisk (se punkt 5.2).

(3) Om behandlingsåtgärden eller projektet är internationellt ska även dataskyddsansvarig delta. Dataskyddsansvarig utför konsekvensbedömning avseende sekretess/ konsekvensbedömning avseende dataskydd för företaget som en mall för lokal konsekvensbedömning avseende sekretess/konsekvensbedömning avseende dataskydd. Lokala dataskyddskrav måste granskas på lokal nivå av lokalt dataskyddsombud. Dataskyddsansvarig granskar även tjänstleverantörerna och/eller utarbetar annan dokumentation/andra mallar (t.ex. sekretessmeddelande). Dataskyddsansvarig informerar dataskyddsombudet om all internationell databehandling i förväg.

(4) Resultatet av konsekvensbedömningen avseende sekretess ska innehålla korrekta detaljer för registren om behandlingsåtgärder. Det obligatoriska innehållet i registren fastställs i artikel 30 av Dataskyddsförordningen. Processägaren är ansvarig för att register skapas. Dataskyddsombudet är ansvarigt för processen för att underhålla registren om behandlingsåtgärder.

## 5.2 Konsekvensbedömning avseende dataskydd (DPIA)

(1) Processägaren ansvarar för utförandet av en konsekvensbedömning avseende dataskydd. Konsekvensbedömningen avseende dataskydd måste involvera dataskyddsombud och lokal säkerhetskoordinator (och eller dataskyddsansvarig/informationssäkerhetschef för internationella projekt) samt ytterligare intressenter (t.ex. arbetsråd, IT-arkitekt(er), juridiska avdelningen osv.).

(2) Konsekvensbedömning avseende dataskydd är en process för att identifiera och minimera dataskyddsriskerna för en behandlingsåtgärd, dvs. för ett projekt. Konsekvensbedömning avseende dataskydd är obligatoriskt enligt Dataskyddsförordningen vid behandling som sannolikt medför en hög risk för individer. Detta inkluderar några särskilda behandlingstyper, men det är också god praxis att göra en konsekvensbedömning avseende dataskydd för alla större projekt som kräver behandling av personuppgifter. En konsekvensbedömning avseende dataskydd krävs vid:

- Användning av ny teknik.
- Automatisk behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer.
- Behandling i stor omfattning av känsliga personuppgifter.
- Behandling av brottslig verksamhet.
- Systematisk övervakning av en allmän plats i stor omfattning osv.

(3) Konsekvensbedömning avseende dataskydd måste:

- Beskriva typ, omfattning, sammanhang och syften med behandlingen.
- Bedöma nödvändighet, proportionalitet och efterlevnadsåtgärder.
- Identifiera och bedöma risker för individer.
- Identifiera eventuella ytterligare åtgärder för att begränsa dessa risker.

För att bedöma risknivån måste PHOENIX-företaget beakta både sannolikheten och allvarligheten av eventuell påverkan på individer. Hög risk kan vara en följd av antingen en hög sannolikhet för viss skada eller en lägre risk för allvarlig skada.

(4) Dataskyddsombudet ska samråda med den lokala datainspektionen om en konsekvensbedömning avseende dataskydd visar att behandlingen skulle leda till en hög risk för de registrerades fri- och rättigheter om inte den personuppgiftsansvarige vidtar åtgärder för att minska riskerna.

# 6. Avtal med tjänstleverantörer

## 6.1 Regler för personuppgiftsbiträdets engagemang

(1) Tjänstleverantören betraktas som personuppgiftsbiträde, om leverantören agerar på uppdrag av och endast på instruktioner från PHOENIX-företaget.

(2) Om PHOENIX-företaget beslutar att använda en tjänst som rör databehandling av ett personuppgiftsbiträde, måste ett databehandlingsavtal (DPA) ingås. För koncernintern databehandling gäller en särskild mall och rutin för databehandlingsavtal.

(3) Om personuppgiftsbiträdets databehandlingsavtal avviker från den lokala mallen eller företagsmallen för databehandlingsavtal, måste den slutliga versionen godkännas av dataskyddsombudet eller den juridiska avdelningen. Granskningen ska initieras av processägaren.

(4) En integrerad del av databehandlingsavtalsförhandlingen är översynen av tjänstleverantörens/personuppgiftsbiträdets TOM. Denna översyn av leverantörens TOM ska fastställa att de följer Dataskyddsförordningen, framför allt med avseende på datasäkerhet (art. 32 Dataskyddsförordningen). Denna kontroll samordnas av dataskyddsområdet med stöd av den lokala säkerhetskoordinatorn.

(5) Dataskyddsavtalet måste ingås skriftligen och dokumenteras.

(6) Det ska ske en regelbunden revision av de tjänstleverantörer som betraktas som personuppgiftsbiträden. I revisionsplanen för dataskydd för tjänstleverantören (inkl. revisionsperioden) ska den sekretessrisk som är relaterad till behandlingsåtgärden övervägas. Minimiperioden för revision är 24 månader. Dataskyddsombud och lokal säkerhetskoordinator ska stödja processägaren under revisionen. Planen för dataskyddsrevision hör till implementeringsåtgärderna (se kapitel 10).

## 6.2 Regler om dataöverföring utanför EU

(1) Dataskyddsförordningen begränsar överföringar av personuppgifter utanför EU/EES, såvida inte de registrerades rättigheter skyddas på annat sätt, eller ett av ett begränsat antal undantag i Dataskyddsförordningen gäller.

(2) PHOENIX-företaget måste alltid känna till hela leveranskedjan (vilket företag/vilket land/vilken tjänst/vilken datakategori). PHOENIX-företaget måste garantera att nivån på dataskyddet efterlever Dataskyddsförordningen i hela behandlingskedjan.

(3) Adekvat skyddsnivå i för ett land/en leverantör utanför EU/EES säkerställs sedan genom vissa garantier som är fördefinierade i Dataskyddsförordningen (t.ex.):
- Kommissionens beslut om adekvat skydd
- Bindande företagsregler
- EU:s standarddataskyddsklausuler osv.

(4) Typen av garanti ska användas som kriterium för val av leverantör. Kommissionens beslut om adekvat skydd ska betraktas som en tillförlitlig garanti. Det bör noteras att

respektive beslut om adekvat skydd kan skilja sig åt i omfattning från land till land. De bindande företagsreglerna kan också ses som en annan stark garanti.

(5) Dataskyddsområdet ska involveras i varje dataöverföring/databehandling utanför EU/EES i förväg.

(6) PHOENIX-företaget ska bevara bevisen för dataöverföring till alla leverantörer utanför EU/EES.

### 6.3 Regler för andra tjänstleverantörer

Alla externa tjänstleverantörer och entreprenörer, som direkt får tillgång till de informationstillgångar, inklusive personuppgifter eller som står under direkt kontroll av PHOENIX group, måste enligt avtal vara skyldiga att följa denna policy och omfattas av sekretess.

## 7. Fullgörande av de registrerades rättigheter

(1) Dataskyddsförordningen ger individer följande rättigheter:

a) **rätten att bli informerad**
Den registrerade ska få relevant information vid tillfället för uppgiftsinsamlingen eller vid första möjliga tillfälle.

b) **rätten till tillgång**
Den registrerade har rätt att begära bekräftelse på om uppgifter som rör honom/henne behandlas och, om så är fallet, begära information angående dessa uppgifter enligt art. 15 i Dataskyddsförordningen.

c) **rätten till rättelse**
Den registrerade har rätt att begära att oriktiga uppgifter rörande honom/henne skall rättas.

d) **rätten till radering**
Den registrerade har rätt att kräva att hans/hennes personuppgifter ska raderas om det inte finns några rättsliga skyldigheter att behålla dem.

e) **rätten att begränsa behandlingen**
Den registrerade kan har rätt att kräva begränsning av behandlingen i enlighet med art. 18 av Dataskyddsförordningen.

f) **rätten till dataportabilitet**
Den registrerade har rätt att begära en kopia av de personuppgifter PHOENIX-företaget innehar om honom/henne och får dessutom begära att den överförs till andra personuppgiftsansvariga.

g) **rätten att invända**
Den registrerade har rätt att när som helst göra invändningar mot behandling av personuppgifter rörande honom eller henne, i synnerhet vid behandling för direkt marknadsföring, profilering och forskningsändamål.

(2) PHOENIX-företaget ska genom lämpliga tekniska och/eller organisatoriska åtgärder säkerställa att företaget kan uppfylla de registrerades rättigheter. Åtgärderna måste dokumenteras.

*Exempel: IT-system ska väljas eller utformas på ett sådant sätt att alla uppgifter som rör en registrerad kan skrivas ut för att uppfylla rätten till tillgång, eller också måste en rutin tillämpas för att säkerställa att alla uppgifter som rör en person kan hämtas manuellt ur systemet.*

(3) Om en registrerad kontaktar PHOENIX-företaget och hävdar en registrerades rättighet, ska den berörda medarbetaren omedelbart vidarebefordra begäran till dataskydds-ombudet och/eller följa de ytterligare lokala reglerna.

## 8. Dataskydd per design

I den mån standardinställningar för databehandling kan göras i ett system, måste dessa inställningar göras på ett sådant sätt att man med tanke på användningsändamålen inte behöver fler uppgifter än nödvändigt, inte längre än nödvändigt och att de inte behandlas mer omfattande än nödvändigt samt att åtkomst för tredje part begränsas så långt det är möjligt.

## 9. Rapportering av dataintrång

### 9.1 Intern rapportering

(1) Varje intrång i personuppgifter måste omedelbart rapporteras till dataskyddsombudet:
a) via portalen för PHOENIX group:
https://phoenixgroup-databreach.integrityplatform.org/
ELLER
b) via det lokala verktyget/förfarandet.
*Exempel:*

- *Förlust av en företagsmobil/företagsdator eller datamedia*
- *Korrespondens till fel mottagare*
- *Obehörig åtkomst till kundportalen eller Speakap*
- *Infektion i systemet av skadlig kod med inverkan på personuppgifter*

(2) Dataskyddsombudet och den lokala säkerhetskoordinator ska skapa ett gemensamt förfarande för att säkerställa rapporteringen. Dataskyddsombudet och den lokala säkerhetskoordinator ansvarar tillsammans för kännedomen om rapportering om dataintrång i PHOENIX-företaget.

(3) Dataskyddsansvarig ska involveras om dataintrånget är internationellt eller stort (hög sekretessrisk för registrerade eller juridisk risk för PHOENIX group).

### 9.2 Hantering av dataintrång

(1) Baserat på den interna rapporten ska dataskyddsombudet identifiera ansvarig(a) person(er)/avdelning(ar). De ansvariga medarbetarna/cheferna bildar en tillfällig arbetsgrupp med uppgifts dataskyddsombudet. I ett kritiskt fall deltar även kommunikationsavdelningen och styrelsen i arbetsgruppen.

(2) Arbetsgruppen undersöker fakta i ärendet och bedömer risken för berörda registrerade (kunder, medarbetare osv.) och för PHOENIX-företaget.

(3) Arbetsgruppen beslutar om möjliga åtgärder för att minska riskerna och om anmälan till tillsynsmyndigheten och/eller den eller de registrerade. Detta beslut måste fattas inom tidsfristen på 72 timmar (från kännedom om dataintrånget) och följa detta protokoll:

| PHOENIX-företaget är/är inte skyldigt att göra en officiell anmälan: | | |
|---|---|---|
| INGEN RISK för den registrerade<br>= Ingen skyldighet att anmäla | RISK för den registrerades rättigheter<br>= Anmälan till tillsynsmyndighet inom 72 timmar | HÖG RISK för den registrerades rättigheter<br>= Anmälan till tillsynsmyndighet inom 72 timmar<br>= Anmälan till den registrerade inom 72 timmar eller utan onödigt dröjsmål. |
| Arbetsgruppen måste i samtliga fall dokumentera dataintrånget. | | |

(4) Styrelsen ska informeras om detta beslut av dataskyddsombudet. Dataskyddsombudet följer den lokala tillsynsmyndighetens regler för anmälningar.

(5) Dataskyddsombud och lokal säkerhetskoordinator skapar ett gemensamt detaljerat förfarande för att säkerställa hantering av dataintrång på lokal nivå.

# 10. Implementeringsåtgärder

## 10.1 Implementeringsåtgärder inom företaget

(1) De koncernomfattande policyerna, företagets dataskyddsstandarder och företagsmallarna representerar de huvudsakliga implementeringsåtgärderna för företagsdataskyddet.

(2) Policyn som skapas av företagsdataskyddet är ett dokument som beskriver specifika krav eller regler som måste uppfyllas, som har godkänts av styrelsen.

(3) Företagsdataskyddsstandarden är inte en policy utan en åtgärd, en process eller ett verktyg för minsta standardåtgärd som har skapats eller tillhandahålls av företagsdataskyddet för att följa dataskyddspolicyn (**Standard**). Koncernledningens godkännande krävs inte. Standarden påverkar inte policyn utan är policyns implementeringsverktyg.

(4) Samlingen av företagsdataskyddsstandarder utgör guiden för skydd av företagsdata (**CDP-guide**).

(5) Dataskyddsansvarig utarbetar den slutliga standarden genom samråd med berörda företagsintressenter och/eller dataskyddsombud, vid behov. Dataskyddsansvarig publicerar standarden för dataskyddsombudet och involverade företagsintressenter. Dataskyddsombuden och de involverade intressenterna ansvarar för ytterligare publicering eller vidarebefordran av standarden till relevanta mottagarna.

(6) Följande intressenter identifieras på koncernnivå för koncernomfattande policy- eller företagsdataskyddsstandarder (beroende på ämne):

- Informationssäkerhetschef
- Företagsarkitekt
- Informationschefens kontor
- Juridiska avdelningen
- Revisionsavdelningen
- Inköp
- HR-avdelningen

(7) PHOENIX-företaget ska tillämpa standarden på lämpligt sätt (t.ex. lokal policy, instruktion, teknisk justering) med beaktande av de rättsliga eller organisatoriska lokala särdragen. Lokal anpassning får göras, men får inte medföra att dataskyddsnivån sjunker under standarden. De lokala sekretessreglerna eller tekniska lösningarna måste alltid representera bästa möjliga dataskydd och på ett adekvat sätt skydda de registrerades sekretess. Dataskyddsombudet rapporterar till dataskyddsansvarig om den lokala implementeringen i landsrapporterna årligen eller på begäran.

(8) Företagsmallen representerar bästa praxis för dataskyddet i PHOENIX group.

## 10.2 Koncept för skydd av företagsdata

De viktigaste implementeringsåtgärderna utgör följande koncept för skydd av företagsdata (**Företagskoncept**). Dataskyddsombudet ska använda detta företagskoncept för egna åtgärder och lokala implementeringsåtgärder:

| Typ av dokument | Dokumentets/verktygets namn |
|---|---|
| **Policy**<br>***(regler som måste uppfyllas)*** | • **Koncernomfattande dataskyddspolicy för PHOENIX group**<br>• **Ytterligare koncernomfattande policyer om dataskydds-ämnen, vid behov**<br>• **Informationssäkerhetspolicyer (säkerställande av personuppgifternas integritet och konfidentialitet).**<br>*Godkänt av koncernledningen*<br>*Även del av det lokala konceptet* |
| **Avtal om koncerndatabehandling och avtal om personuppgiftsansvarig för koncernen** | • **Resultat av den koncerninterna förhandlingen**<br>*Godkänt av koncernledningen och den lokala styrelsen*<br>*Även del av det lokala konceptet* |
| **Standarder för skydd av företagsdata** ***(minimistandard för åtgärd, process eller verktyg i PHOENIX group)*** | **Exempel**<br>• Standard för internationell dataöverföring<br>• Standard för livscykel för dataskyddskonceptet:<br>• Standard för konsekvensbedömning avseende dataskydd<br>• Standard för lagringskoncept<br>• Rapporteringssystem för dataintrång<br>• Plattform för koncernens onlineutbildning |
| **Medvetenhet** | Kampanj medvetenhet inom koncernen |

## 10.3 Lokalt dataskyddskoncept

(1) De lokala implementeringsåtgärderna utgör det lokala dataskyddskonceptet (Lokalt koncept). Dataskyddsombudet stöder styrelsen i arbetet med att definiera innehållet i det lokala konceptet. Ramverket för det lokala konceptet är följande:

| Typ av dokument | Dokumentets/verktygets namn |
|---|---|
| **Lokala policyer/SOP/instruktion** | Lokal dataskyddspolicy (vid behov)<br>Lokal reglering som baseras på CDP-guiden eller lokala juridiska krav:<br>• Förordning om konsekvensbedömning avseende sekretess/konsekvensbedömning avseende dataskydd<br>• Förordning om lagringskoncept<br>• Förordning om hantering/rapportering av dataintrång<br>• Förordning om upprätthållande av register över behandlingsåtgärder<br>• Förordning om utövande av de registrerades rättigheter |
| **Lokala mallar** | Baserat på företagsmallarna<br>• Databehandlingsavtal<br>• Checklistor för ett sekretessmeddelande<br>• Flygblad |
| **TOM** | • Koncernomfattande eller lokala informations-säkerhetspolicyer<br>• Formell och informell dokumentation (t.ex. säkerhets-kopior av koncept, loggfiler osv.) |
| **Medvetenhet** | Lokal utbildning och medvetenhetskampanj |