# Riktlinjer för dataskydd och Dataskyddspolicy för Reiling-koncernen

# Innehållsförteckning

## I. Syftet med riktlinjerna för dataskydd

Som en del av vår sociala medvetenhet och vårt sociala ansvar har Reiling-koncernen åtagit sig att följa internationella lagar om dataskydd. Upprätthållande av dataskydd är grundläggande för en pålitlig och trovärdig affärsrelation och är av yttersta vikt för ett utmärkt rykte som en attraktiv leverantör av sysselsättning.

Riktlinjerna för dataskydd utgör en av de nödvändiga grundförutsättningarna för överföring av uppgifter[1] inom Reiling-koncernen. Riktlinjerna garanterar också den nödvändiga nivån av dataskydd som krävs enligt den europeiska dataskyddsförordningen[2] och nationella lagar för gränsöverskridande dataöverföring, även i länder där ingen sådan nivå av dataskydd är nödvändig enligt lag[3] .

## II. Tillämpningsområde och ändringar av riktlinjerna för dataskydd

Riktlinjerna för dataskydd gäller för alla bolag inom Reiling-koncernen, dvs. för alla beroende bolag som ingår i Reiling-koncernen, samt för koncernbolag och deras anställda. Riktlinjerna för dataskydd omfattar behandling av alla personuppgifter[4] . Anonymiserade uppgifter[5] , t.ex. för statistisk analys eller forskning, omfattas också av dataskyddsriktlinjerna.

De enskilda företagsgrupperna har inte rätt att införa bestämmelser som på något sätt avviker från dataskyddsriktlinjerna. Ändringar i riktlinjerna för dataskydd kan endast göras i samråd med dataskyddsansvarig. Ändringarna kommer omedelbart att rapporteras till Reiling-koncernen inom ramen för det förfarande som anges för ändringar av riktlinjer.

Den aktuella versionen av dataskyddsriktlinjerna finns under dataskyddsinformation på Reiling-koncernens webbplats på www.reiling.de.

## III. Tillämpning av delstatlig lagstiftning

Denna riktlinje för dataskydd införlivar den globala acceptansen av dataskyddsprinciper utan att ersätta befintlig nationell lagstiftning, den kompletterar respektive nationella dataskyddslagar. Respektive nationell lag har företräde om den kräver avvikelser från dessa riktlinjer för dataskydd eller ställer mer omfattande krav. Innehållet i dataskyddsriktlinjerna ska följas även om det inte finns någon motsvarande nationell lag.

Varje bolag inom Reiling-koncernen ansvarar för att följa dataskyddsriktlinjerna och sina rättsliga förpliktelser. Om något företag har anledning att tro att rättsliga skyldigheter strider mot de skyldigheter som

---

[1] Se XV

[2] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för enskilda personer med avseende på behandling av personuppgifter, om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning GDPR) finns på http://eur-lex.europa.eu/legal-content/DE/TET/?uri=CELEX:3201GR0679

[3] Se XV

[4] Se XV

[5] Se XV

anges i riktlinjerna för dataskydd, måste det berörda företaget omedelbart informera dataskyddsansvarig utan dröjsmål. I händelse av en konflikt mellan nationell lagstiftning och dataskyddsriktlinjerna kommer Reiling GmbH & Co. KG arbeta tillsammans med den berörda företagsgruppen för att hitta en rimlig lösning i enlighet med målen i riktlinjerna för dataskydd.

## IV. Principer för behandling av personuppgifter

### 1. Laglighet

Vid behandling av personuppgifter måste den registrerades[6] personliga rättigheter beaktas och respekteras. Personuppgifter måste samlas in och behandlas på ett lagligt sätt.

### 2. Begränsning av syftet

Behandlingen av personuppgifter får endast ske för de ändamål som fastställdes innan uppgifterna samlades in. Ändringar av ändamålen i efterhand är endast möjliga i begränsad omfattning och kräver motivering.

### 3. Öppenhet

Den berörda personen måste informeras om hanteringen av hans / hennes uppgifter. I princip måste personuppgifterna samlas in från de berörda personerna själva. När uppgifterna samlas in bör den berörda personen åtminstone kunna uppfatta eller informeras om följande:

- Den personuppgiftsansvariges identitet och kontaktuppgifter[7]
- Kontaktuppgifter till dataskyddsansvarig
- Syftet med databehandlingen och dess rättsliga grund
- Tredje parter[8] eller kategorier av tredje parter till vilka uppgifterna kan komma att överföras.
- Den planerade lagringens varaktighet, t.ex. kriterierna för att fastställa den.
- Den lagliga rätten till information från personuppgiftsbiträdet om de berörda personuppgifterna, samt rätten till rättelse, radering, begränsning av behandling, invändning mot behandling och slutligen rätten till dataportabilitet.
- Rätt att överklaga till en tillsynsmyndighet.
- Huruvida tillhandahållandet av personuppgifter krävs enligt lag eller avtal eller är nödvändigt för att fullgöra ett avtal, huruvida den berörda registrerade är skyldig att tillhandahålla de begärda personuppgifterna och vilka de möjliga konsekvenserna skulle bli om så inte sker.

[6] Se XV
[7] Se XV
[8] Se XV

### 4. Undvikande av data och datareduktion

Innan personuppgifter behandlas ska det kontrolleras om och i vilken utsträckning detta är nödvändigt[9] för att uppnå det avsedda ändamålet med behandlingen. Anonymiserade och statistiska uppgifter ska användas i rimlig utsträckning när så är möjligt. Personuppgifter får inte sparas för eventuella framtida syften.

### 5. Radering

Personuppgifter som inte längre behövs på grund av att lagstadgade och affärsprocessrelaterade lagringstider har löpt ut måste raderas. Om det finns indikationer på legitimt dataskydd i ett enskilt fall måste uppgifterna sparas tills detta har klarlagts juridiskt.

### 6. Faktiska uppgifter och uppgifternas aktualitet

Personuppgifter ska hållas korrekta, fullständiga och vid behov uppdaterade. Lämpliga åtgärder måste vidtas för att säkerställa att felaktiga, ofullständiga eller föråldrade uppgifter raderas, korrigeras, kompletteras eller uppdateras.

### 7. Konfidentialitet och databehandling

Datakonfidentialitet gäller för personuppgifter. Alla uppgifter måste behandlas konfidentiellt och skyddas genom lämpliga organisatoriska och tekniska åtgärder mot obehörig åtkomst, olaglig behandling eller utlämnande, oavsiktlig förlust, ändring eller förstörelse.

## V. Legitimitet för behandling av uppgifter

Insamling, behandling och användning av personuppgifter är endast tillåten om någon av följande omständigheter föreligger. Ett sådant tillstånd krävs också om avsikten med insamlingen, behandlingen och användningen av personuppgifterna på något sätt ska ändras från de ursprungliga omständigheterna.

### 1. Uppgifter om kunder och partners

**1.1 Databehandling för ett kommersiellt/avtalsmässigt förhållande**

Personuppgifter om den berörda parten, befintlig kund eller partner, kan behandlas och användas för att motivera genomförandet av och villkoren för ett avtal. Detta omfattar även stöd från avtalspartnern, i den mån detta är relevant för avtalets syfte. Under förberedelserna för ett avtal, dvs. under avtalets inledningsfas, får behandlingen av personuppgifter för att förbereda alla erbjudanden eller för att uppfylla andra önskemål från den berörda parten som syftar till att ingå ett avtal kontaktas under inledningsfasen med hjälp av de uppgifter som de har tillhandahållit. Eventuella begränsningar som den berörda parten har uttryckt måste följas. Följande krav enligt V. 1.2 måste uppfyllas för reklamåtgärder som går utöver detta.

[9] Se XV

### 1.2 Databehandling för marknadsföringsändamål

Om den berörda personen kontaktar ett företag inom Reiling-koncernen med en begäran om information (t.ex. begäran om informationsmaterial om en viss produkt), är databehandling tillåten/behörig för att uppfylla denna begäran.

Kundrelationer och reklamkampanjer kräver ytterligare rättsliga krav. Uppgifter för reklamändamål eller marknads- och opinionsundersökningar är tillåtna, förutsatt att detta är förenligt med det syfte för vilket uppgifterna ursprungligen samlades in. Den registrerade ska informeras om användningen av uppgifterna för reklamändamål. Om uppgifter samlas in uteslutande för reklamändamål är det frivilligt för den berörda personen att lämna information. Den berörda personen måste också informeras om att det är frivilligt att lämna uppgifter för detta ändamål och om sin rätt att när som helst återkalla denna information. Som en del av kommunikationen med den berörda personen måste den registrerades samtycke[10] till behandling av deras uppgifter för reklamändamål erhållas. Den berörda personen bör kunna välja mellan de olika tillgängliga kontaktkanalerna, t.ex. post, e-post och telefon inom ramen för samtycket.

(se medgivande V. 1.3)

Om den registrerade motsätter sig att uppgifterna används för reklamändamål är vidare användning av uppgifterna inte tillåten och måste frysas för dessa ändamål. Dessutom finns det i vissa länder restriktioner för användning av uppgifter för reklamändamål.

### 1.3 Samtycke till databehandling

Databehandling kan ske på grundval av den berörda personens samtycke. Innan samtycke ges måste den registrerade informeras i enlighet med IV.3 i dessa riktlinjer för dataskydd och informeras om sin rätt att när som helst återkalla detta samtycke. Av juridiska skäl måste samtycket inhämtas skriftligen eller via e-post.

### 1.4 Databehandling baserad på lagligt tillstånd

Behandling av personuppgifter är också tillåten om det krävs eller är tillåtet att behandla personuppgifter enligt nationella bestämmelser. Typen och omfattningen av databehandlingen måste vara nödvändig för den lagligt tillåtna databehandlingen och baseras på denna lagbestämmelse.

### 1.5 Databehandling baserad på berättigat intresse

Behandling av personuppgifter kan också ske om det är nödvändigt för att tillgodose ett berättigat intresse hos ett eller flera bolag inom Reiling-koncernen. Berättigade intressen är vanligtvis av juridisk natur (t.ex. verkställighet av utestående betalningar) eller kommersiella (t.ex. förebyggande av avtalsbrott). Behandling av personuppgifter som grundar sig på ett berättigat intresse får inte ske om det i det enskilda fallet finns en indikation på att den berörda personens skyddsintressen väger tyngre än intresset av behandlingen. De intressen som kräver skydd måste granskas före behandlingen.

[10] Se XV

### 1.6 Behandling av skyddsvärda uppgifter

Behandling av särskilt känsliga uppgifter[11] får endast ske om detta krävs enligt lag eller om den berörda personen har gett sitt samtycke till detta förfarande. Behandling av dessa uppgifter är också tillåten om det är absolut nödvändigt för att hävda eller försvara rättsliga anspråk mot den registrerade. Om behandling av skyddsvärda uppgifter planeras måste dataskyddsansvarig informeras i förväg.

### 1.7 Automatiserat individuellt beslutsfattande

Automatiserad behandling av personuppgifter för bedömning av individuella egenskaper (t.ex. arbetsansökningar) får inte vara den enda grunden för beslut med negativa rättsliga följder eller betydande nackdelar/handikapp för den berörda personen. De som berörs måste informeras om faktum och resultatet av automatiserat individuellt beslutsfattande och ges möjlighet att kommentera. För att undvika felaktiga beslut måste en övervaknings- och verifieringsinspektion säkerställas och utföras av en anställd.

### 1.8 Användardata och internet

Om personuppgifter samlas in, behandlas och/eller används på webbplatser eller i appar ska den berörda registrerade informeras om detta genom dataskyddsmeddelanden och, i förekommande fall, cookiemeddelanden. Dataskyddsmeddelandena och, i förekommande fall, cookiemeddelandena ska integreras på ett sådant sätt att de är lätt identifierbara och omedelbart tillgängliga för den berörda personen.

Om en användarprofil skapas för att utvärdera användningsbeteendet för webbplatser och appar (spårning), måste de berörda informeras genom dataskyddsmeddelanden. Personlig spårning får endast ske om nationell lagstiftning tillåter detta eller om den berörda personen har gett sitt samtycke till förfarandet. Om spårning ska ske under pseudonym ska de berörda personerna ges möjlighet att invända mot detta i ett dataskyddsmeddelande (opt-out).

Om åtkomst till personuppgifter möjliggörs på webbplatser eller appar i ett område som är föremål för registrering, måste identifiering och autentisering av de berörda personerna utformas på ett sådant sätt att lämpligt skydd uppnås för respektive åtkomst.

## 2 Personaluppgifter.

### 2.1 Databehandling för anställningsförhållanden

För anställningsförhållandet får personuppgifter som är nödvändiga för att upprätta, genomföra och avsluta anställningsavtalet behandlas. När ett anställningsförhållande inleds får den sökandes personuppgifter behandlas. Efter avslag måste den sökandes uppgifter raderas, med beaktande av tidsfrister för bevisning, såvida inte den sökande har samtyckt till fortsatt lagring för en efterföljande urvalsprocess. Samtycke krävs också för att uppgifterna ska kunna användas för ytterligare ansökningsförfaranden eller innan ansökan vidarebefordras till en annan grupp inom företaget.

[11] Se XV

I ett befintligt anställningsförhållande måste databehandlingen alltid vara relaterad till syftet med anställningsavtalet, såvida inte något av följande tillstånd för databehandling träder in.
Om det krävs att ytterligare information om den sökande inhämtas från tredje part när anställningsförhållandet inleds eller i ett befintligt anställningsförhållande, ska hänsyn tas till nationella rättsliga krav. I händelse av osäkerhet måste den berörda personens samtycke inhämtas.
För behandling av personuppgifter som sker inom ramen för anställningsförhållandet men som inte ursprungligen tjänar till att fullgöra anställningsavtalet måste en rättslig legitimation lämnas i varje enskilt fall. Det kan röra sig om lagstadgade krav, medarbetarens samtycke eller företagets berättigade intressen.

**2.2 Databehandling baserad på lagligt tillstånd**

Behandlingen av personuppgifter om anställda är också tillåten om den statliga lagstiftningen kräver, kräver eller tillåter databehandlingen. Databehandlingens art och omfattning måste vara nödvändig för den lagligt tillåtna databehandlingen och grunda sig på dessa rättsliga bestämmelser. Om det finns ett rättsligt utrymme för spelrum eller flexibilitet måste den anställdes intressen beaktas och skyddas.

**2.3 Samtycke till databehandling**

Behandling av uppgifter om anställda får ske med stöd av samtycke från den berörda personen. Förklaringar om samtycke måste ges frivilligt. Ett ofrivilligt samtycke är ogiltigt. Av bevisskäl måste samtyckesförklaringen alltid inhämtas skriftligen eller elektroniskt. Innan samtycke ges måste den registrerade informeras i enlighet med IV.3 i dessa riktlinjer för dataskydd och göras medveten om sin lagliga rätt att när som helst återkalla sitt givna samtycke.

**2.4 Databehandling baserad på legitima intressen**

Behandling av personuppgifter om anställda kan också ske om det är nödvändigt för att tillgodose ett berättigat intresse hos ett företag inom Reiling-koncernen. Berättigade intressen är vanligtvis juridiska (t.ex. hävdande, genomförande eller försvar av rättsliga anspråk) eller ekonomiskt motiverade (t.ex. värdering av företag).
Behandling av personuppgifter med stöd av intresseavvägning får inte ske om det i det enskilda fallet finns anledning att anta att arbetstagarens skyddsvärda intressen väger tyngre än företagets intresse av behandlingen. Förekomsten av berättigade intressen som kräver skydd måste utvärderas för varje behandling.
Kontrollförfaranden som kräver behandling av uppgifter om anställda får endast genomföras om det finns en rättslig skyldighet eller ett berättigat skäl till detta. Om det finns ett berättigat skäl måste kontrollförfarandets proportionalitet granskas. Företagets berättigade intressen vid genomförandet av kontrollförfarandena (t.ex. efterlevnad av rättsliga bestämmelser och interna företagsregler) måste noggrant vägas mot ett eventuellt berättigat intresse hos den anställde som påverkas av förfarandena, sådana förfaranden får endast genomföras om de är lämpliga. Företagets berättigade intresse och skyddet av alla berörda medarbetares eventuella berättigade intressen måste fastställas, vägas och dokumenteras innan något förfarande inleds. Dessutom måste ytterligare krav som finns enligt nationell lagstiftning (t.ex. informationsrättigheter för den berörda registrerade) beaktas.

**2.5 Behandling av särskilda kategorier av personuppgifter**

Särskilda kategorier av personuppgifter får endast behandlas under vissa förutsättningar. Särskilda kategorier av personuppgifter är uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening samt behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. Enligt nationell rätt kan även andra uppgiftskategorier klassificeras som sådana som kräver särskilt skydd, eller så kan innehållet i uppgiftskategorierna definieras på annat sätt. På samma sätt får uppgifter som rör brott endast behandlas under särskilda villkor som utfärdats och fastställts i nationell lagstiftning.

Behandlingen måste vara uttryckligen tillåten eller föreskriven i statlig lag. Dessutom kan behandling vara tillåten om det är nödvändigt för att det ansvariga organet ska kunna uppfylla arbetstagarnas rättigheter och skyldigheter på det arbetsrättsliga området. Den berörda arbetstagaren kan också frivilligt uttrycka sitt samtycke till behandlingen.

Om behandling av mycket konfidentiella uppgifter planeras, måste dataskyddsombudet informeras i förväg.

**2.6 Automatiserat individuellt beslutsfattande**

Om personuppgifter som rör ett anställningsförhållande behandlas automatiskt för att bedöma individuella egenskaper (t.ex. i samband med urval av personal eller bedömning av förmåga och skicklighet), får sådan automatisk behandling inte vara den enda grunden för beslut som får negativa konsekvenser eller betydande nackdelar för den berörda arbetstagaren. Den berörda arbetstagaren måste informeras om fakta och resultatet av det automatiserade individuella beslutsfattandet och ges möjlighet att kommentera.

**2,7 Telekommunikation och internet**

Telefonsystem, e-postadresser, intranät och internet samt interna nätverk för sociala medier tillhandahålls i första hand av företaget inom ramen för de operativa arbetsuppgifterna. De är arbetsverktyg och företagsresurser. De får användas inom ramen för gällande lagbestämmelser och företagets juridiska riktlinjer.

Vid tillåten användning för privata ändamål måste sekretessen för telekommunikationer och tillämplig nationell telekommunikationslagstiftning respekteras i den mån de är tillämpliga.

Det förekommer ingen allmän övervakning av telefon- och e-postkommunikation eller av åtkomst till internet och intranät. För att avvärja eventuella angrepp på IT-infrastrukturen eller på enskilda användare kan skyddsåtgärder vidtas vid gränssnitten till nätverket hos de enskilda bolagen inom Reiling-koncernen, vilka blockerar tekniskt skadligt innehåll eller analyserar angreppsmönster. Av säkerhetsskäl får användningen av telefonsystem, e-postadresser, intranät och internet samt interna sociala nätverk endast loggas och övervakas under en begränsad tidsperiod. Utvärdering av dessa personuppgifter får endast ske vid en konkret motiverad misstanke om lagöverträdelse. Sådana kontroller får endast utföras av auktoriserade utredningsavdelningar eller kvalificerad godkänd personal, som omfattas av proportionalitetsprincipen. Respektive nationella lagar ska följas på samma sätt som befintliga bestämmelser inom Reiling-koncernen.

## VI. Överföring av personuppgifter

Överföring av personuppgifter till mottagare inom eller utanför Reiling-koncernen omfattas av kravet på tillåtlighet för behandling av personuppgifter enligt avsnitt V. Mottagaren av sådana uppgifter måste åläggas att endast använda dessa personuppgifter för angivna ändamål.
Vid överföring av uppgifter till en mottagare utanför Reiling-koncernen i ett tredje land[12] måste nivån på dataskyddet motsvara riktlinjerna för dataskydd inom Reiling-koncernen och ska garanteras.
Vid överföring av uppgifter från tredje part till Reiling-koncernen måste det säkerställas att uppgifterna kan användas för de avsedda ändamålen.

## VII. Avtalshantering

Uppdragsbehandling sker när en uppdragstagare (personuppgiftsbiträde) får i uppdrag att behandla personuppgifter utan att ta ansvar för tillhörande affärsprocesser. I sådana fall ska ett avtal om uppdragsbehandling träffas mellan både de externa uppdragstagarna och bolagen inom Reiling-koncernen. Det uppdragsgivande företaget behåller det fulla ansvaret för att databehandlingen genomförs på ett korrekt sätt. Uppdragstagaren får endast behandla personuppgifter enligt uppdragsgivarens instruktioner. Vid tilldelning av kontraktet måste följande krav uppfyllas; och den behöriga uppdragsavdelningen måste säkerställa genomförandet.

1. Uppdragstagaren ska utses på grundval av sina kvalifikationer och sin förmåga att garantera de tekniska och organisatoriska skyddsåtgärder som krävs.
2. Avtalet ska lämnas in skriftligen. Riktlinjerna för databehandling samt beställarens och uppdragstagarens ansvar ska dokumenteras.
3. De avtalsnormer som redan har tillhandahållits av dataskyddsombudet måste tillämpas.
4. Kunden måste övertyga sig om att uppdragstagaren uppfyller sina skyldigheter innan han påbörjar databehandlingen. En entreprenör kan verifiera efterlevnaden av datasäkerheten genom att lämna in motsvarande certifiering. Beroende på risken med databehandlingen kan verifieringen behöva upprepas regelbundet under avtalsperioden.
5. Vid gränsöverskridande uppdragsbehandling måste respektive nationella krav för överföring av personuppgifter till utlandet uppfyllas. I synnerhet får behandling av personuppgifter från Europeiska ekonomiska samarbetsområdet (EES) endast äga rum i ett tredjeland om uppdragstagaren kan bevisa en nivå av dataskydd som är likvärdig med befintligt dataskydd. Lämpliga instrument kan vara följande:
    a. Avtal om EU:s standardavtalsklausuler för uppdragsbehandling i tredje land tillsammans med uppdragstagaren och eventuella underleverantörer.
    b. Uppdragstagaren deltar i ett av EU erkänt certifieringssystem för att skapa en lämplig nivå av dataskydd.

[12] Se XV

c. Erkännande av bindande företagspolicyer hos uppdragstagaren för att tillhandahålla en adekvat nivå av dataskydd av de ansvariga tillsynsmyndigheterna för dataskydd.

## VIII. Den berörda partens lagliga rättigheter.

Varje registrerad person kan göra anspråk på följande rättigheter. Utövandet av dessa rättigheter måste omedelbart utföras av den ansvariga avdelningen och får inte leda till några nackdelar för den berörda personen.

1. Den registrerade kan begära information om sina personuppgifter, uppgifternas art och i vilket syfte uppgifterna lagras. Om anställningsförhållandet ger ytterligare omfattande rätt till tillgång till arbetsgivarens dokument (t.ex. personalakter) enligt respektive arbetslagstiftning, ska detta inte påverkas.
2. Om personuppgifter överförs till tredje part måste information om mottagarens identitet och kategorisering lämnas ut. Om personuppgifter ska överföras till en mottagare i ett tredjeland eller en internationell organisation ska den berörda personen informeras om de lämpliga skyddsåtgärder som berättigar till att uppgifterna överförs.
3. Om personuppgifterna är felaktiga eller ofullständiga kan den registrerade begära att uppgifterna rättas och/eller kompletteras.
4. Den registrerade kan invända mot att hans/hennes personuppgifter behandlas för reklamändamål eller marknads- och konsumentundersökningar. Under sådana omständigheter kan samtycket också återkallas när som helst. I sådana fall måste uppgifterna blockeras.
5. Den registrerade har rätt att begära radering eller begränsning av sina uppgifter om den rättsliga grunden för behandlingen av uppgifterna inte längre finns eller har upphört att existera.
   Detsamma gäller om syftet med databehandlingen har upphört på grund av att tiden har gått ut eller av andra giltiga skäl. Befintliga lagringsskyldigheter och skyddsvärda intressen som står i konflikt med radering måste beaktas.
6. Den berörda personen/den registrerade har en grundläggande rätt att invända mot behandlingen av hans eller hennes uppgifter, vilket måste beaktas om hans eller hennes berättigade intressen väger tyngre än intresset av behandlingen på grund av en särskild personlig situation. Detta gäller dock inte om lagbestämmelser kräver att behandlingen utförs.
7. Den registrerade har också rätt att få information om de personuppgifter som rör honom eller henne och som han eller hon har lämnat.
8. Den registrerade har rätt att bli informerad om sin rätt att lämna in ett klagomål till de ansvariga tillsynsmyndigheterna.
9. Den registrerade har rätt att få all tillgänglig information om varifrån hans eller hennes personuppgifter härrör.

## IX. Konfidentiell behandling

Personuppgifter omfattas av datasekretess. Det är förbjudet för medarbetare att obehörigen samla in, bearbeta eller använda sådana uppgifter. Obehörig behandling är all slags behandling som utförs av en anställd utan att ha anförtrotts att göra det inom ramen för hans eller hennes arbetsuppgifter och utan att vara behörig att göra det. Behovsprincipen gäller, det vill säga att medarbetare endast får ha tillgång till personuppgifter om och i den utsträckning som det är nödvändigt för deras respektive roller och uppdrag. Detta kräver en noggrann och korrekt fördelning och åtskillnad av roller och ansvarsområden samt administration och underhåll av dessa inom ramen för behörighetsbegrepp.
Medarbetarna får inte använda personuppgifter för sina egna privata eller kommersiella intressen. Det är också strängt förbjudet att överföra personuppgifter till obehöriga parter eller att göra dem tillgängliga för dem på något sätt. Arbetsgivaren måste informera sina anställda om den lagstadgade skyldigheten att spara uppgifter i början av anställningsförhållandet. Denna lagstadgade skyldighet kvarstår även efter det att anställningen har upphört.

## X. Säkerhet vid bearbetning

Personuppgifter måste alltid skyddas mot obehörig åtkomst, olaglig behandling, utlämnande och förlust, förfalskning eller förstörelse. Detta gäller oavsett om uppgifterna behandlas elektroniskt eller i pappersform. Innan nya databehandlingsförfaranden införs, i synnerhet nya IT-system, måste tekniska och organisatoriska åtgärder för skydd av personuppgifter definieras och genomföras. Dessa åtgärder måste baseras på teknicknivån, de risker som antas före behandlingen och kraven på skydd av uppgifterna (skyddsklassificering som anges i register över behandlingsaktiviteter). Den berörda avdelningen kan rådfråga informationssäkerhetsansvarig (ISO), dataskyddssamordnaren eller dataskyddschefen. De tekniska och organisatoriska åtgärderna för att skydda personuppgifter är en del av Reiling-koncernens informationssäkerhetshantering och måste därför ständigt uppdateras för att möta alla tekniska och organisatoriska innovationer och ändringar.

## XI. Övervakning av dataskydd

Efterlevnaden av riktlinjerna för dataskydd och tillämpliga lagar om dataskydd granskas regelbundet genom dataskyddsrevisioner och andra övervakningskällor. Genomförandet av de senare är en angelägenhet och ett ansvar för dataskyddschefen, dataskyddssamordnarna och alla andra anställda med revisionsbehörighet samt utsedda externa revisorer. Dataskyddschefen måste informeras om alla resultat av dataskyddsövervakningen. Reiling GmbH & Co. KG (holdingbolag) rådgivande styrelse ska informeras om alla betydande resultat inom ramen för respektive rapporteringsskyldighet. På begäran görs resultaten av dataskyddsövervakningen tillgängliga för de ansvariga tillsynsmyndigheterna för dataskydd. De relevanta dataskyddsmyndigheterna kan också utföra sin egen övervakning av efterlevnaden av bestämmelserna i direktivet inom ramen för sina befogenheter enligt nationell lagstiftning.

## XII. Incidenter som rör uppgiftsskydd

Vid överträdelse av riktlinjerna för dataskydd eller andra skyddsbestämmelser (dataskyddsincident[13] ) måste alla medarbetare omedelbart informera sin respektive chef eller dataskyddschef. Den chef som är ansvarig för funktionen eller enheten är skyldig att omedelbart informera den ansvariga dataskyddssamordnaren eller dataskyddschefen om eventuella dataskyddsincidenter.

I händelser av

- olaglig överföring av personuppgifter till tredje part
- tredje parts olagliga tillgång till personuppgifter
- eller i händelse av förlust av personuppgifter

de anmälningar som föreskrivs i företaget (Reiling anmälan om dataskyddsincident) måste göras omedelbart så att befintliga rapporteringsskyldigheter för dataskyddsincidenter kan uppfyllas enligt nationell lagstiftning.

## XIII. Ansvar och påföljder

Ledningen för koncernens företag är ansvariga och redovisningsskyldiga för databehandling inom sina respektive ansvarsområden. De är därför skyldiga att se till att de lagstadgade kraven på dataskydd och de som finns i riktlinjerna för dataskydd beaktas (t.ex. nationella registreringskrav). Det är en ledningsuppgift för cheferna att säkerställa korrekt databehandling i enlighet med dataskyddet genom organisatoriska, personalmässiga och tekniska åtgärder. Ansvaret för att dessa krav uppfylls ligger hos respektive medarbetare. I händelse av myndighetskontroll av dataskyddet måste dataskyddsansvarig omedelbart informeras.
Respektive ledning och fabrikschef för Reiling-koncernen som inte är baserad i Tyskland utan inom Europa, måste utse en dataskyddssamordnare till dataskyddschefen. Organisatoriskt bör denna uppgift utföras i samarbete med dataskyddschefen. Dataskyddssamordnarna är kontaktpersoner på plats för dataskydd. De kan också utföra övervakning och kontroller och är skyldiga att se till att alla anställda känner till innehållet i riktlinjerna för dataskydd. Respektive ledning är skyldig att stödja dataskyddschefen och dataskyddssamordnarna i deras arbete. De som ansvarar för affärsprocesser och projekt måste i förväg informera dataskyddssamordnarna om varje ny behandling av personuppgifter. Vid databehandlingsprojekt som kan leda till särskilda risker för den registrerades personliga rättigheter måste dataskyddschefen involveras innan behandlingen påbörjas. Detta gäller särskilt för särskilda kategorier av personuppgifter. Cheferna måste se till att alla deras anställda får nödvändig utbildning i dataskydd. Felaktig behandling av personuppgifter eller andra överträdelser av dataskyddslagstiftningen är straffbara i många länder och kan även leda till skadeståndskrav. Överträdelser som enskilda medarbetare är ansvariga för kan leda till arbetsrättsliga sanktioner.

[13] Se XV

## XIV. Dataskyddsansvarig för Reiling-koncernen

Dataskyddschefen, som fungerar som ett internt oberoende organ, arbetar för att säkerställa efterlevnaden av nationella och internationella skyddsbestämmelser. Han ansvarar för riktlinjer för dataskydd och övervakar deras genomförande. Dataskyddschefen utses av VD eller den juridiska representanten för Reiling GmbH & Co. KG. Dataskyddssamordnarna ska omedelbart informera dataskyddschefen om eventuella dataskyddsrisker.

Alla berörda registrerade kan kontakta dataskyddschefen eller den dataskyddssamordnare som är ansvarig för honom/henne med förslag, frågor, begäran om information eller klagomål i samband med dataskydds- eller datasäkerhetsfrågor. Förfrågningar och klagomål kommer på begäran att behandlas konfidentiellt.

Om respektive dataskyddssamordnare inte kan lösa ett klagomål, stoppa eller åtgärda en överträdelse av riktlinjerna för dataskydd, måste han eller hon rådfråga dataskyddschefen. De beslut som fattas av dataskyddschefen för att åtgärda överträdelser av dataskyddet måste beaktas av den verkställande ledningen. Förfrågningar från tillsynsmyndigheter ska ställas till dataskyddschefen.

Dataskyddschefen kan kontaktas på följande sätt:

Ansvarig för dataskydd. Reiling GmbH &Co. KG, Bussemasstraße 49, 33427 Marienfeld

E-post: datenschutzbeauftragten@reiling.de ; datenschutz@reiling.de

## XV. Definitioner

- **En adekvat och lämplig nivå av dataskydd** i tredje land erkänns av EU-kommissionen om kärnan i integritetsskyddet, som det ser ut i EU:s medlemsländer, förstås och skyddas på ett väsentligt sätt. EU-kommissionen tar hänsyn till alla omständigheter kring en dataöverföring eller en specifik kategori av dataöverföringar när den fattar sitt beslut. Detta inkluderar även en bedömning av nationell lagstiftning samt respektive etiska regler och säkerhetsåtgärder.
- **Uppgifter anonymiseras** om en personlig referens inte längre kan fastställas av någon. Till exempel om en personlig referens endast skulle kunna återupprättas med en orimligt stor insats i form av tid, kostnader och arbetskraft.
- **Särskilt känsliga uppgifter** är uppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, genetiska uppgifter, biometriska uppgifter i syfte att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning. Enligt nationell lagstiftning kan ytterligare uppgiftskategorier klassificeras som uppgifter som kräver särskilt skydd, eller så kan innehållet i uppgiftskategorierna skilja sig åt. Dessutom får uppgifter som rör brott ofta endast behandlas under särskilda villkor som fastställs i nationell lagstiftning.
- **Den registrerade** i den mening som avses i denna riktlinje om dataskydd är varje fysisk person från vilken uppgifterna behandlas. I vissa länder kan även juridiska personer beröras.
- **Dataskyddsincidenter** är alla händelser där det finns en motiverad misstanke om att personuppgifter har eller skulle kunna få olaglig åtkomst, exponering, kopiering, överföring, radering eller användning. Detta kan även avse åtgärder som vidtas av tredje part eller av anställda.
- **En tredje part** är någon annan än den registrerade och det organ som ansvarar för databehandlingen. Personuppgiftsbiträden är inte tredje part inom EU när det gäller dataskyddslagstiftning, eftersom de enligt lag är tilldelade det ansvariga organet.
- **Tredjeländer** inom ramen för dataskyddsdirektivet är alla länder utanför Europeiska unionen / EES. Undantag är de stater vars skyddsnivå har erkänts som tillräcklig och godtagbar av EU-kommissionen.
- **Med samtycke** avses varje slag av frivillig, specifik, informerad och otvetydig viljeyttring genom vilken den registrerade, genom ett uttalande eller en tydligt bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.
- **Behandlingen av personuppgifter är nödvändig** om den lagliga avsikten eller det berättigade intresset inte kan uppnås utan de aktuella personuppgifterna eller endast kan uppnås med oproportionerligt stora ansträngningar.
- **Europeiska ekonomiska samarbetsområdet (EES)** är en ekonomisk zon som är associerad med EU och där Norge, Island och Liechtenstein är medlemmar.
- **Personuppgifter** är all slags information som rör en identifierad eller identifierbar fysisk person ("den registrerade"); en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras, särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, lokaliseringsuppgifter, en onlineidentifierare eller en eller flera faktorer som är specifika för den

fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

- Med **behandling** avses varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter eller uppsättningar av personuppgifter, vare sig det sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, begränsning, radering eller förstöring.
- **Personuppgiftsansvarig** är det juridiskt oberoende företaget inom Reiling-koncernen, vars affärsverksamhet initierar respektive behandlingsåtgärd.