DATASKYDDSPOLICY

Kvartselektronik AB 556691-9043

Med anledning av den nya dataskyddsförordningen (EU:s gemensamma datalagstiftning, GDPR, General Data Protection Regulation) som träder i kraft 25 maj 2018 upprättas denna dataskyddspolicy.

Personuppgiftsansvarige:

Personuppgiftsansvarige för bolaget är den juridiska personen Kvartselektronik AB 556691-9043.

Personuppgiftsbiträde:

Personuppgiftsbiträde för bolaget är bolagets VD, Per Svensson.

Dataskyddsombud:

Dataskyddsombud har inte utsetts då bolaget inte behandlar personuppgifter i sin kärnverksamhet eller känsliga personuppgifter i stor omfattning.

Bolagets verksamhet

Bolaget arbetar huvudsakligen inom försäljning och distribution av elektronik komponenter. Produkterna säljs i huvudsak till B2B kunder i Sverige och Europa.

Dataskyddshistorik

Bolaget har aldrig haft något dataintrång eller att personuppgifter har läckt obehörigen.

Personuppgifter som bolaget hanterar

Bolaget har identifierat de personuppgifter som hanteras till följande:
- Kontaktpersoner hos kunder och leverantörer som är juridiska personer
- Anställda

Dessa uppgifter hanteras i bolaget på digital väg, dels i affärssystemets register och dels i löne-programmet samt via epost. Dataskyddsförordningen omfattar även manuell behandling som medför att personuppgifter finns i ett register som är sökbart, dataskyddsförordningen artikel 2. Bolaget hanterar inte kund- och leverantörskontakter manuellt i fysiska register. För de anställda finns årsvisa lönepärmar som är sökbara per månad och således också omfattas av dataskyddsförordningen. Av bolagets 7 anställda har alla tillgång till bolagets affärssystem och register.
Känsliga personuppgifter som är särskilt skyddade har i dataskyddsförordningen artikel 9 identifierats som följande:

- ras eller etniskt ursprung
- politiska åsikter,
- religiös eller filosofisk övertygelse
- medlemskap i fackförening
- behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person,
- uppgifter om hälsa

- uppgifter om en fysisk persons sexualliv eller sexuella läggning

Bolaget hanterar två av dessa känsliga uppgifter avseende sina anställda och det är medlem i fackförening som generar avdrag på lön avseende fackavgifter samt uppgifter om hälsa i de fall det påverkar utbetalning av lön genom sjukintyg. Beträffande kunder och leverantörskontakter hanteras endast s.k. okänsliga personuppgifter såsom namn, leveransadress, epost och telefon.

Syfte med lagring av personuppgifter – laglig grund

Bolaget anser att man har laglig grund för de register med personuppgifter som hanteras i enlighet med dataskyddsförordningen, artikel 6, då behandlingen är nödvändig för att fullfölja avtal i vilka den registrerade är part. För att kunna fullfölja de affärsavtal som ingås med bl.a garantitider måste bolaget ha tillgång till rätt kontaktuppgifter. Beträffande register över anställda grundar de sig på anställningsavtal.

Personuppgifterna i bolagets register lämnas inte ut till tredje part utöver kontrolluppgifter för anställda som lämnas till myndigheter och pensionsbolag för att fullgöra arbetsrättsliga skyldigheter.

Personuppgifter i ostrukturerat material

De personuppgifter som bolaget hanterar i ostrukturerat material är epost. Datainspektionen anser att personuppgifter av okänslig karaktär i sedvanlig epostkorrespondens mellan kollegor och andra vardagliga meddelanden inte kräver att tredje person skall informeras.

Epost med känsliga personuppgifter skickas alltid via Microsoft Outlook ”kryptera meddelande”. Om bolaget erhåller epost som innehåller känsliga personuppgifter görs bedömning om uppgifterna behöver bevaras och förs då över i aktuella digitala register och eposten raderas. De fall då känsliga personuppgifter skickas via epost rör uteslutande anställda, som har informerats om att de i möjligaste mån skall undvika känsliga uppgifter via epost alternativt skicka krypterat. Lönespecifikationer och kontrolluppgifter skickas via löneprogrammet Visma 600 till ”Mitt lönebesked”. Kontrolluppgifter för lön till Skatteverket och Försäkringskassan skickas digitalt via myndigheternas egna portaler. Avtalsrättsliga krav på kontrolluppgifter för lön till pensionsbolag lämnas via bolagens portaler eller via traditionell post. All mottagen epost som besvaras länkar till bolagets integritetspolicy.

Krav på samtycke

Med utgångspunkt i de okänsliga personuppgifter som bolaget registrerar på kund- och leverantörskontakter räcker det enligt dataskyddsförordningen att informera de berörda att vi har uppgifterna registrerade och att vederbörande har tillgång till uppgifterna. Något explicit samtycke krävs inte.

Bolaget har uppdaterat sina kund- och leverantörsregister med aktuella kontaktuppgifter och i samband med det gjort epostutskick till de kontakter som finns i bolagets register för att tillgodose deras rättigheter enligt dataskyddsförordningen. De har informerats om de uppgifter som bolaget registrerar, namn, leveransadress, telefon, epost, bolagets gallringstid samt att registren är helt interna och inte lämnas ut till tredje part. Likaså informerades de om möjligheten till radering ur systemen med vissa begränsningar, dvs om bolaget måste ha uppgifterna för att kunna fullfölja affärsavtal. Vid nya kontakter informeras om allt ovan.

Inventering

Bolaget har inventerat hela sin verksamhet och upprättat en **behörighetsstruktur** (bilaga 1) över de aktuella register som hanterar personuppgifter. Där framgår vem eller vilka som har tillgång till de olika registren i respektive system. Likaså framgår hur länge bolaget arkiverar uppgifter innan de gallras.
Bolaget har även uppdaterat sin **systemdokumentation** (bilaga 1) innehållande bolagets fysiska datakomponenter, systemskiss över databaser, programvaror, epost samt nätverksanslutningar.
I inventeringen ingår även en sammanställning av de **externa konsulter** (bilaga 1) som bolaget har IT-lösningar med samt hur de i sin tur säkerställer att dataskyddsförordningen efterföljs.
Bolaget har även inventerat affärssystemet möjlighet till privacy by design, dvs att systemet styr användaren rätt och begränsar möjligheten till att registrera bl.a. personnummer och känsliga uppgifter. Affärssystemet Pyramid har inga enkla begränsningar av fritext på kund och leverantör, men bolaget har aldrig tidigare registrerat känsliga uppgifter och de anställda har informerats om att så heller inte skall ske i framtiden. Vid årlig gallring kontrolleras kund- och leverantörsregister för att säkerställa att känsliga uppgifter inte har lagt till.

Personuppgifter i anställdas datorer

I bolaget sparas inte personuppgifter i de enskilda anställdas datorer utan hanteras i bolagets lokala nätverk. Alla anställda har informerats om att en arbetsgivare har rätt att följa upp att dataskyddsförordningens regler följs och därmed kan komma att kontrollera den anställdes dator.

Externa Konsulter

Bolaget samarbetar med WiigData som handhar bolagets server och mailserver.
Se deras behörighetsstruktur, bilaga 1.

Gallring

Personuppgiftsbiträdet ansvarar för att gallring sker manuellt genom årlig genomgång av aktuella register där uppgifter gallras bort och register i pappersformat kasseras via destruktion.

Utbildning

Samtliga anställda på bolaget har informerats om den nya dataskyddsförordningen och dess innebörd för deras egen del samt tagit del av denna dataskyddspolicy med bilagor.

Risk- och sårbarhetsanalys

Utifrån bolagets systemstruktur (bilaga 2) gör bolaget analysen att de tekniska lösningar bolaget har i relation till typen personuppgifter bolaget hanterar är ett fullgott skydd mot dataintrång och obehörigt utlämnande av uppgifter. Med behörighetsstrukturen (bilaga 1) som grund har bolaget infört de rutiner som i möjligaste mån skall minimera risken att bolaget utsätts för dataintrång eller att personuppgifter utelämnas till obehörig person.

Personuppgiftsincident

Om bolaget skulle utsättas för ett dataintrång har bolaget infört rutiner där personuppgiftbiträdet omedelbart skall dokumentera incidenten och inom 72 timmar anmäla händelsen till tillsynsmyndighet om incidenten kan medföra risker för den enskildas fri- och rättigheter. Likaså skall den eller de berörda informeras om incidenten kan leda till allvarliga risker såsom diskriminering, id-stölder, bedrägerier eller finansiella stölder.