eqoweb©	**HS Copy&Media Service AB** Betongvägen 40 973 45 Luleå 0920-227070	**Rutin för GDPR (Dataskyddsförordningen)** **inkl Personuppgiftsbiträdesavtal (principen)**	**F008-45**
		Godkänd av:	VD
		Datum	28.02.2019

Rutin för GDPR

General Data Protection Regulation = Dataskyddsförordningen

Syfte:
Att företagets ledningssystem/datasystem skall fungera i enlighet med GDPR
Omfattning:
Tillämpliga processer, händelser och aktiviteter i ledningssystemet
Ansvar/befogenheter:
VD ansvarar för hela verksamheten
GDPR- ansvarige på företaget ansvarar för rutinens genomförande

Rutinbeskrivning:

1. Företaget ska utse en ansvarig för GDPR och denne ska äga kunskap om GDPR författningen Förteckning av ansvarig personal finns i F004-01
2. Företaget ska teckna personuppgiftsbiträdesavtal med de företag som hanterar företagets personuppgifter
3. Kartlägg: Hitta alla personuppgifter
   All behandling av personuppgifter måste följa GDPR. Då gäller det att veta:
   1. Vilka personuppgifter har vi? För Eqoweb systemet har vi personuppgifter kopplade till olika arbetsuppgifter/ roller i ledningssystemet.
      Dessa är förtecknade i F004-01
   2. Vad gör vi med dem?
      Personuppgifterna är kopplade till olika arbetsuppgifter i ledningssystemet, i övrigt används inte uppgifterna
   3. Vilken laglig rätt stödjer vi oss på vid olika behandlingar
      Uppgifter i ledningssystemet är kopplad till anställning eller uppdrag i ledningssystemet
   4. Vem har tillgång till personuppgifterna?
      Eqoweb´s konsulter (inkl datastöd) = läs- och redigeringsmöjlighet Systemansvariga på företaget = läs- och redigeringsmöjlighet
      Medarbetare på företaget = läs möjlighet
   5. När raderar vi dem?
      När rollen/ arbetsuppgifterna upphör eller anställningen upphör.
      Kontroll av att rätt personuppgifter finns i systemet görs och dokumenteras årligen i samband med LGG (egen punkt på dagordningen)
4. Skapa en Dataskyddspolicy (F003-03)
   Beskriv vad ni vill och hur ni tänker göra
5. Bygg kultur och börja städa
   1. Informera personalen om GDPR
   2. Besluta om generella principer för städningen och vika personuppgifter som ska behållas och varför
6. Informera mera - Gör det så alla förstår
   Detta berör mera dataverksamheten utåt mot kunder, leverantörer, användare och besökare
   Informationen kan tex vara...
   1. Vem du/företaget är
   2. Syfte, det vill säga vad du ska ha uppgifterna till
   3. Vilken rättslig grund du stödjer dig på
   4. När du kommer att ta bort uppgifterna

5. Om du tänker dela med någon och om du delar med någon utanför EU/EES. (T ex Google, Microsoft)
6. Vilka rättigheter den registrerade har
7. Lite annat smått och gott.
   Du hittar den kompletta listan över informationskrav i Dataskyddsförordningens artikel 13.
   I praktiken är det ganska enkelt. Beställer man något via företagets sidor på internet så ska informationen finnas där. Om man beställer något via post eller telefon så kan man skicka med informationen med orderbekräftelsen, fakturan eller leveransen.
   Om man har en enkel verksamhet och en bra dataskyddspolicy så kanske allt redan är på plats.

   Det är företagets bedömning att godkännande av coockies inkl datasäkerhets-policy vid inloggning täcker GDPRs krav, dock har alla företag skyldighet att kontrollera vad som gäller för det egna företaget i detalj
8. När det är möjligt så ska informationen lämnas innan man samlar in uppgifterna. Om det inte är möjligt så ska man göra det så snart som möjligt, senast vid första kontakttillfället.

7. Dokumentera: Samla bevis
   1. Säkerställ genom notering i protokoll vid ex vis personalmöte att information om GDPR genomförts. Särskild utbildning i GDPR kan med fördel noteras.
   2. Vid LGG noteras de åtgärder som företaget genomfört för att säkerställa att GDPR uppfylls.

8. **Personuppgiftsbiträdesavtal (principen)**
   Den som är ansvarig för behandling av personuppgifter är också ansvarig för sina underleverantörer. Verktyget för att behålla kontrollen heter personuppgifts-biträdesavtal.
   Den här texten innehåller inte juridiska råd. Den är en översiktlig presentation av några enstaka delar av lagen. Texten har som mål att ge en enkel introduktion eftersom många företag påverkas och behöver ta ställning till om man behöver söka juridisk rådgivning.

   Den ansvarige
   Den som bestämmer att personuppgifter ska samlas in och vad de ska användas till är personuppgiftsansvarig i lagens mening. Med ansvaret följer skyldigheter att värna uppgifterna, att informera den registrerade samt andra skyldigheter GDPR ålägger. Det är organisationen eller företaget som får denna roll, inte de anställda som utför uppgifterna. Den ansvarige är alltid 100 procent ansvarig. Det går inte att dela på detta ansvar.
   Biträdet
   Ofta har den som behandlar personuppgifter en underleverantör som man för över uppgifter till. Det kan vara en datahall, en mail-leverantör, ett kreditupplysningsföretag eller annan part. En sådan part kallas personuppgiftsbiträde. Kom ihåg att den som är personuppgiftsansvarig har det fulla ansvaret hela tiden.
   Avtalet
   För att stödja den ansvarige kräver GDPR att om man delar data med någon annan, till exempel en underleverantör, måste det finnas ett avtal som binder underleverantören till att följa lagens krav. Det är detta som är ett personuppgiftsbiträdesavtal. Låt oss kalla det ”biträdesavtal” i den här texten.
   Enligt GDPR ska biträdesavtalet reglera att biträdet:
   Bara behandlar personuppgifter enligt dokumenterad instruktion.

Se till att alla som behandlar uppgifterna har åtagit sig att iaktta konfidentialitet.
Upprätthåller en anpassat hög säkerhetsnivå såväl med rutiner som i utrustning.
Låter den ansvariga godkänna eventuella underbiträden samt tecknar biträdesavtal om biträde anlitas.
Bistår den ansvariga när någon registrerad vill utnyttja sina rättigheter.
Bistår den ansvariga kring säkerhet, dataintrång och andra skyldigheter.
Radera eller återlämna data vid avtalets upphörande.
Ge den ansvariga möjlighet att kontrollera att biträdet fullföljer sina skyldigheter ovan.

Underbiträden

Det gamla ordspråket ”Min dräng har också en dräng” var kanske lite roligt en gång i tiden men idag är det snarare regel än undantag. Många varor och tjänster levereras som slutprodukt via en lång kedja av underleverantörer. Man kan säga att ordspråket ”Skomakare, bli vid din läst” har fått en renässans. Var och en gör det den är bäst på. Allt annat köper man in.

Underbiträdesavtal

Om man har rätt att använda ett underbiträde så ska man teckna ett biträdesavtal mellan sig själv som biträde och underbiträdet. Principen för det avtalet är samma som för det vanliga biträdesavtalet