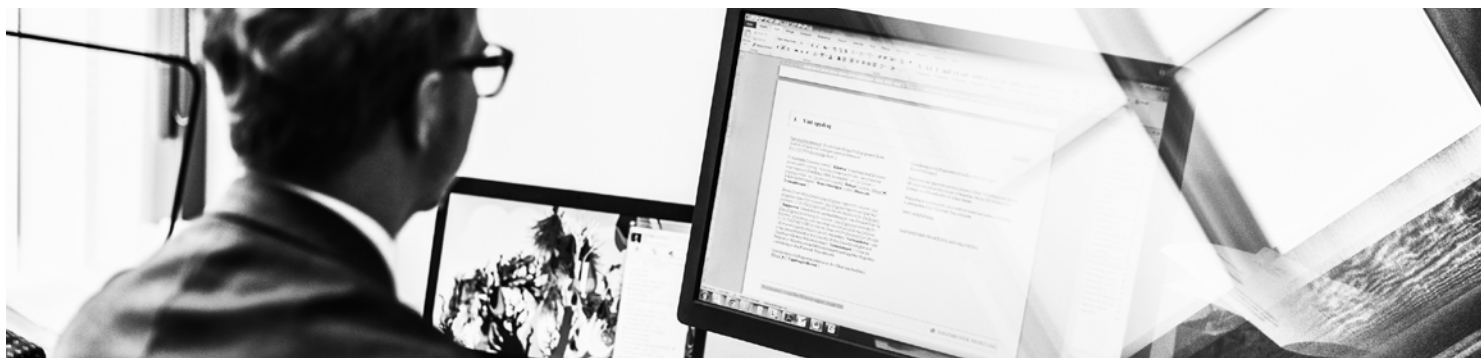


Personuppgifter



KONTAKTPERSONER

STOCKHOLM
Erica Wiking Häger
erica.wiking.hager@msa.se

Anders Bergsten
anders.bergsten@msa.se

GÖTEBORG
Niklas Sjöblom
niklas.sjoblom@msa.se

WWW.MANNHEIMERSWARTLING.SE

Nya striktare regler för behandling av personuppgifter

I januari 2012 publicerade EU kommissionen ett förslag till ny dataskyddsförordning i syfte att skapa enhetliga dataskyddsregler inom hela EU och för att därigenom underlätta för företag att verka på den inre marknaden.

Efter ett långt lagstiftningsarbete inom EU nåddes i januari 2016 en politisk överenskommelse och i april 2016 antogs den nya dataskyddsförordningen. Företag har nu två år på sig att anpassa sig innan förordningen den 25 maj 2018 ska börja att tillämpas i samtliga medlemsstater. Samtidigt upphävs den nu gällande svenska personuppgiftslagen (PUL).

Regeringen har tillsatt en utredning som ska föreslå hur övrig svensk lagstiftning på dataskyddsområdet behöver anpassas till förordningen. Utredningen ska presentera sitt förslag i maj 2017. Vi räknar med att utredningen kommer att leda till att förordningen kompletteras med viss lokal svensk lagstiftning, till exempel rörande behandling av anställdas personuppgifter.

Vad innebär förordningen för företag?

Förordningen innehåller många nyheter och förändringar, bland annat väsentligt ökade compliance-krav för företag och höga sanktionsavgifter vid bristande regel efterlevnad. Några av de viktigaste nyheterna är:

SAMMA REGLER GÄLLER INOM HELA EU

Idag baseras lagstiftningen på ett direktiv och varje medlemsstat har sin egen lagstiftning rörande behandling av personuppgifter. Det innebär att företag med verksamhet i olika medlemsstater måste beakta lokala regler i varje land. Eftersom de nya reglerna genomförs i form av en förordning kommer det – i princip – att vara samma regler som gäller i samtliga medlemsstater.



”ONE-STOP SHOP”

Företag kommer under de nya reglerna enbart att behöva ha kontakt med en dataskyddsmyndighet, nämligen myndigheten i det land där koncernen har sitt huvudkontor. För bolag med huvudkontor i Sverige är det Datainspektionen som blir tillsynsmyndighet för hela koncernens verksamhet.

ÖKADE KRAV PÅ INTERN DOKUMENTATION

Förordningen kräver att företag kan visa att de uppfyller förordningens bestämmelser. Detta kan till exempel ske genom personuppgiftspolicys och uppförandekoder. Företag måste även föra en intern förteckning över alla sina personuppgiftsbehandlingar. Ett företag måste, på Datainspektionens begäran, kunna presentera sin interna dokumentation rörande hur företaget behandlar personuppgifter.

ETT STARKARE SKYDD FÖR INDIVIDEN

Individens rättigheter stärks genom förordningen. Företag kommer bland annat att behöva lämna utförligare information om hur man hanterar personuppgifter. Individens ges även en rätt att ”bli glömd”, vilket betyder att företag under vissa förutsättningar kan bli skyldiga att radera all information man har sparat om en individ.

RISK- OCH SÄRBARHETSANALYSER

Förordningen kräver att företag genomför en risk- och sårbarhetsanalys innan man initierar behandlingar som skulle kunna medföra stora integritetsrisker för individer, exempelvis användande av kameraövervakning och annan övervakning av anställda.

RAPPORTERINGSSKYLDIGHET VID SÄKERHETSINCIDENTER (S.K. DATA BREACH)

Vid säkerhetsincidenter, till exempel om personuppgifter spridits oavsiktligt eller genom dataintrång, måste företaget som huvudregel rapportera händelsen till Datainspektionen inom 72 timmar från det att företaget fick kännedom om händelsen. Dessutom måste företaget, under vissa omständigheter, informera de individer som berörs av säkerhetsincidenten.

UTÖKAT ANSVAR FÖR PERSONUPPGIFTSBITRÄDEN

Personuppgiftsbiträden är företag som behandlar personuppgifter för andra företags räkning, till exempel IT-leverantörer. Personuppgiftsbiträdena får ett utökat ansvar under förordningen. Till exempel måste biträdet föra en egen förteckning över sina behandlingar, genomföra risk- och sårbarhetsanalyser och i vissa fall utse ett personuppgiftsombud. Dessutom kan ett biträde drabbas av administrativa sanktionsavgifter om biträdet inte uppfyller kraven i förordningen.

PERSONUPPGIFTSOMBUD

Många företag kommer att bli skyldiga att utse personuppgiftsombud. Det gäller till exempel företag som behandlar stora mängder känsliga personuppgifter. Dessutom uppställs krav på att personuppgiftsombudet har erforderliga kunskaper om förordningen.

VÄSENTLIGT SKÄRPTA SANKTIONER

Den mest uppmärksammade ändringen är att företag som inte lever upp till förordningens krav, när den träder i kraft den 25 maj 2018, riskerar sanktionsavgifter på upp till 20 000 000 EUR eller upp till 4 % av företagets totala globala årsomsättning.



Hur kan företagen förbereda sig?

Företag har nu två år på sig att inrätta sig efter förordningen. För att säkerställa att ett företag lever upp till förordningens krav behöver företagets nuvarande behandlingar av personuppgifter gås igenom. Vi rekommenderar att företag:

Vi rekommenderar att företag:

- Säkerställer att man har en organisation som kan hantera förordningen och förbereda företaget på de nya kraven samt att vid behov utse ett personuppgiftsombud
- Kartlägger hur företagets befintliga behandlingar ser ut och identifierar sina huvudsakliga dataskyddsrisiker
- Utvärderar (inrättar och uppdaterar) rutiner, policys och övrig dokumentation rörande företagets personuppgiftsbehandlingar
- Särskilt går igenom hur företagen begär in samtycken
- Inrättar gallringsrutiner
- Kartlägger överföringar av personuppgifter till tredje land

Mannheimer Swartlings expertis på personuppgifts-området

Vi har stor erfarenhet av att hjälpa klienter med personuppgiftsfrågor och därmed sammanhängande compliance-projekt. Vårt team, bestående av omkring 20 jurister, hjälper bland annat klienter att kartlägga befintlig personuppgiftshantering, att genomföra risk- och sårbarhetsanalyser, att upprätta personuppgiftspolicys och samtyckeshandlingar, att ta fram rutiner för globala överföringar av personuppgifter samt att genomföra fullständiga compliance-program med översyn av befintliga processer och rutiner. Många av de projekt där vi deltar är globala och vi har därför ett utvecklat nätverk av samarbetspartners med relevant expertis.

Vi hjälper även klienter att genomföra GAP-analyser i förhållande till den nya förordningen. Syftet med analyserna är att skapa en förståelse för vilka de huvudsakliga dataskyddsrisiker är samt att hjälpa klienterna att identifiera och prioritera vilka åtgärder som behöver vidtas för att uppfylla de nya reglerna.

STOCKHOLM
NORRLANDSGATAN 21
BOX 1711
111 87 STOCKHOLM

GÖTEBORG
ÖSTRA HAMNGATAN 16
BOX 2235
403 14 GÖTEBORG

MALMÖ
SÖDERGATAN 22
BOX 4291
203 14 MALMÖ

HELSINGBORG
SÖDRA STORGATAN 7
BOX 1384
251 13 HELSINGBORG

FRANKFURT
BOCKENHEIMER LANDSTRASSE 51-53
60325 FRANKFURT AM MAIN, TYSKLAND

BERLIN
MAUERSTRASSE 83-84
10117 BERLIN, TYSKLAND

MOSKVA
ROMANOV DVOR BUSINESS CENTRE
ROMANOV PER. 4
125009 MOSKVA, RYSSLAND

SHANGHAI
25/F, PLATINUM
NO. 233 TAICANG ROAD, LUWAN DISTRICT
SHANGHAI 200020, KINA

HONGKONG
33/F, JARDINE HOUSE
1 CONNAUGHT PLACE
CENTRAL, HONGKONG, KINA

BRYSSEL
IT TOWER
AVENUE LOUISE 480
1050 BRYSSEL, BELGIEN

NEW YORK
101 PARK AVENUE
NEW YORK NY 10178, USA

WWW.MANNHEIMERSWARTLING.SE

Mannheimer Swartling är Nordens ledande affärsjuridiska byrå. Bland våra klienter finns framstående svenska och internationella företag och organisationer. Byrån arbetar brett, både när det gäller typ av uppdrag och geografi. Verksamheten bedrivs genom elva kontor i sex länder – Sverige, Tyskland, Ryssland, Kina, USA och Belgien – samt i nära samarbete med andra framstående internationella byråer.



**MANNHEIMER
SWARTLING**