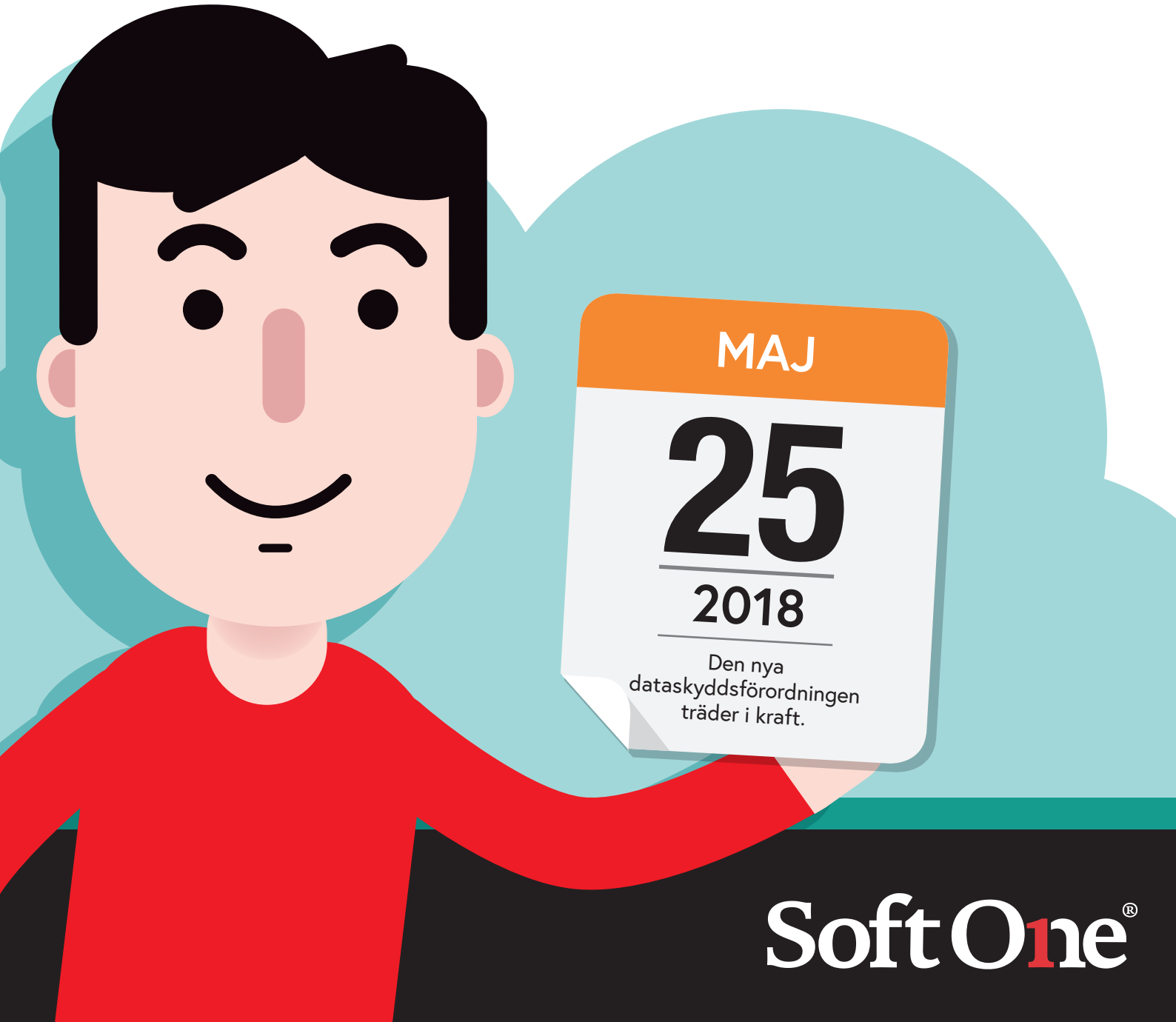
Hantera nya dataskyddsförordningen GDPR

ENKLA GRUNDER I DATASKYDD



SoftOne®

GDPR

Den nya dataskyddsförordningen GDPR träder i kraft 25 maj 2018 och ersätter då den svenska personuppgiftslagen PUL.

GDPR (General Data Protection Resolution) är ett EU-direktiv, som i Sverige konkretiseras i den så kallade dataskyddsförordningen. Vi får en gemensam EU-lagstiftning som reglerar hur personuppgifter får behandlas.

Den främsta skillnaden är att företag inte längre kan äga personuppgifter, utan endast låna dem för ett specifikt ändamål.

Den nya lagen kan upplevas som lite luddig. Praxis kommer att växa fram i takt med att lagen börjar tillämpas. I Sverige ansvarar Datainspektionen för att lagen efterlevs.

Vid överträdelse kan företaget dömas till böter på upp till 4 % av omsättningen. Det här tvingar företag att fundera över hur de hanterar och skyddar personuppgifter.

VI GER DIG EN ENKEL GRUNDKURS I DATASKYDD.

Tre grundregler i företagets vardag

1. SAMLA BARA TILL BESTÄMT ÄNDAMÅL
Samla inte in fler personuppgifter än nödvändigt – och bara för ett specifikt och i förväg bestämt ändamål.

2. INFORMERA MER
När ni samlar in personuppgifter så måste ni informera personen om vilka uppgifter det handlar om och varför ni gör det. Kommer ni att lämna uppgifterna vidare till andra, så måste ni tala om det.

3. SPARA MINDRE
När personuppgiften inte längre behövs för det syfte som de en gång samlades in för, så ska de tas bort. Det betyder till exempel att uppgifter om personer som inte längre är kunder eller leverantörer måste tas bort från IT-systemen.

Tidigare har det varit praxis att personuppgifter om en före detta kund kunnat användas för marknadsföring under ett års tid efter att kundrelationen har upphört. Så är det alltså inte längre.

Vissa personuppgifter kan dock behöva sparas för att t ex säljaren ska kunna fullgöra garantiåtaganden. Uppgifterna sparas då med ett nytt syfte.

OBS!

TÄNK PÅ!
Det kan finnas annan lagstiftning som säger att uppgifter måste sparas en viss tid. Det kan till exempel röra sig om din bokföring, pensionsuppgifter och kontrolluppgifter.

Det här är personuppgifter

ALL INFORMATION SOM KAN KNYTAS TILL EN FYSISK PERSON:

- Personnummer, namn och adress
- Foton på personer
- Ljudinspelningar som lagras elektroniskt kan vara personuppgifter även om det inte nämns några namn i inspelningen.
- Ett organisationsnummer när det handlar om en enskild näringsverksamhet.
- Registreringsnumret på en bil kan vara en personuppgift om det går att knyta till en fysisk person, medan registreringsnumret på en firmabil som används av flera, kanske inte är en personuppgift.

FÅR MAN SPARA UPPGIFTER OM KUNDERS INTRESSEN?

Spelar kunden golf? Har kunden allergier som kan vara bra att känna till inför affärslunchen? För att få registrera detta måste kunden få information om och varför ni kommer att spara uppgiften, och ge sitt godkännande. Uppgiften måste vara relevant för kundrelationen – annars får den inte registreras.

TÄNK PÅ!

Personuppgifter kan finnas i e-post, sociala medier etc. Även historisk information omfattas av GDPR.

OBS!

HUR GÖR VI MED HEMSIDAN OCH NYHETSBREVET?

Enligt GDPR måste du inhämta samtycke från de personer som nämns på företagets hemsida och i nyhetsbrevet.

Men om du ansöker om utgivningsbevis för hemsidan och nyhetsbrevet är det möjligt att fortsätta ha personuppgifter i löpande text. Det gör du hos Myndigheten för press, radio och tv. Du ska även utse en ansvarig utgivare för hemsidan och nyhetsbrevet.

I och med detta lyfts de bort från Dataskyddsförordningen, och blir en yttrandefrihetsfråga. Den ansvariga utgivaren blir då ansvarig för det som skrivs.

Vem ansvarar för vad
i samband med molntjänster?

ALLA FÖRETAG SKA HA ETT REGISTER SOM BESKRIVER HUR MAN HANTERAR PERSONUPPGIFTER.

Här talar ni om vem som är ansvarig för ett visst register eller IT-system, vad det används till, vilka typer av personuppgifter som förekommer samt vilka typer av uppgifter och på vilken rättslig grund uppgifterna hanteras.

NYA ROLLER OCH BEGREPP:

PERSONUPPGIFTSANSVARIG

Den organisation som samlat in person-uppgifter och anlitar en molntjänst-leverantör är personuppgiftsansvarig, och har ansvar för att lagar följs.

DATASKYDDSOMBUD

Dataskyddsombudet är en fysisk person i eller utanför organisationen som kan påpeka brister (som en internrevisor). Ombudet ska anmälas till Datainspektionen.

PERSONUPPGIFTSBITRÄDESAVTAL

Den personuppgifts-ansvariga måste i regel se till att det finns ett personuppgifts-biträdesavtal.

PERSONUPPGIFTSBITRÄDE

Molntjänstleverantören (t ex SoftOne) är personuppgiftsbiträde till den personuppgiftsansvariga.

Både personuppgiftsansvariga och personuppgiftsbiträden ska utse ett dataskyddsombud om:

- personuppgiftsbehandlingen utförs av en myndighet eller ett offentligt organ (dock ej domstolar i deras dömande verksamhet)
- kärnverksamheten består av personuppgiftsbehandling som kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning
- kärnverksamhet består av behandling i stor omfattning av så kallade känsliga person-uppgifter eller brottsuppgifter.

OBS! Den som vill får utse ett dataskyddsombud även i andra fall.

Din molntjänst SoftOne GO ger ett starkt skydd

SKYDDAR MOT DATAINTRÅNG PÅ SERVRAR

SoftOne GO körs på egna servrar i Sverige som är övervakade dygnet runt. De förvaras i säkerhetsklassade datorhallar, med brandväggar, virusskydd m.m. Endast ett fåtal behöriga personer har tillgång till personlig data. Behörigheter styrs av roller med krav på säkra lösenord m.m.

ENKELT ATT FLYTTA PERSONLIG INFORMATION

Individens personliga information ska vara flyttbar mellan olika system. Med SoftOne GO kan den exporteras till XML-format, som sedan kan importeras i de flesta system.

GER TILLGÅNG TILL SAMLAD INFORMATION OM PERSONER

En individ har rätt att se vilken personlig information som finns. SoftOne GO ger enkelt en samlad överblick om vilken information om individen som finns i systemet. Det är också enkelt att uppdatera personinformation i systemet.

RADERA OCH ANONYMISERA

Möjlighet att radera eller anonymisera person-uppgifter, om inte legala krav säger annorlunda.

UNDERLÄTTAR RAPPORTERING VID INCIDENT

All bearbetning av personliga data i SoftOne GO loggas, så att man kan följa om otillbörlig access har skett samt informera individen. Detta kräver att det finns giltiga kontaktuppgifter för varje individ.

SÄKER INLOGGNING

Med inloggning till SoftOne GO via softone.online stödjer SoftOne ditt företags behov av säker lösenordshantering.

Om något ändå inträffar...

OBS!

Om ni råkar ut för en "personuppgiftsincident" ska det rapporteras till Datainspektionen och den person det berör inom 72 timmar.

Exempel på en personuppgiftsincident kan vara ett borttappat USB-minne med personuppgifter, ett dataintrång eller att någon obehörig tagit del av personuppgifter.

Säkerhetstips!

Tänk på att er största säkerhetsrisk faktiskt är den mänskliga faktorn och företagets egna medarbetare som har legal tillgång till data.

- Använd komplexa lösenord och byt dem regelbundet.
- Ha en ”clean desk policy”. Inloggningsuppgifter, USB-minnen och utskrifter ska låsas in när du inte arbetar med dem. Datorn ska alltid låsas när du lämnar den. Använd identifiering för att få ut utskrifter.
- Tänk på vad du mailar och svarar på. Var uppmärksam mot ”phishing mail”.

SOFTONE GROUP ÄR ISO 27001-CERTIFIERADE – FÖR DIN TRYGGHETS SKULL

SoftOne är ISO 27001-certifierade. Det innebär att vi har ett ledningssystem för informationssäkerhet.

Den här certifieringen är extra viktig med tanke på den nya dataskyddsförordningen och ger en trygghet för dig som kund.

Certifieringen garanterar hög informationssäkerhet och innebär att vi bedriver ett kontrollerat, systematiskt informationssäkerhetsarbete i hela organisationen.

CERTIFIERAT ISO 27001 SVENSK CERTIFIERING

DU FÅR EN LEVERANTÖR MED:

- Säkerställd hög kompetens inom IT-säkerhetsområdet för alla anställda.
- Oberoende löpande granskning av säkerhet och rutiner via certifierad IT-säkerhetsrevisor.
- Krav på uppdaterade riskanalyser över viktiga funktioner.

Checklista GDPR

ATT FÅ KLART NU:

- ☐ Gå igenom och dokumentera hur ni behandlar personuppgifter.
- ☐ Undersök säkerheten kring er data idag, oavsett om lagringen sker i IT-system eller i förråd/arkiv.
- ☐ Undersök befintliga IT-system och deras säkerhet. Lokalt installerade system kan utgöra en säkerhetsrisk.
- ☐ Kartlägg om er IT-leverantör har en säker informationshantering och gärna att de är ISO 27001-certifierade.
- ☐ Informera löpande alla delar av organisationen att dessa förändringar är planerade.
- ☐ Ta reda på om din organisation behöver ett dataskyddsombud (DSO). Detta kommer i så fall att vara en central person i hela GDPR-arbetet.
- ☐ Ledningen måste avsätta resurser (tid och pengar) för att genomföra projektet.

ATT TA TAG I SÅ SNART SOM MÖJLIGT:

- ☐ Identifiera hur personuppgifter rör sig genom organisationen (livscykeln).
- ☐ Upprätta avtal med personuppgiftsbiträden och/eller personuppgiftsansvariga.
- ☐ Gå igenom och anpassa alla avtal som rör hantering av personuppgifter.
- ☐ Upprätta policy och regler för säker lösenordshantering.

ATT FÅ KOLL PÅ INFÖR 25 MAJ 2018:

- ☐ Se till att ha rutiner, dokumentation och policys på plats för att följa reglerna.
- ☐ Se till att de dokument som beskriver handhavandet av personuppgifter är uppdaterade och kommunicerade till de anställda.
- ☐ Utbilda organisationen i vad som nu kommer börja gälla.
- ☐ Uppdatera IT-struktur, system och säkerhet och se till att dessa lever upp till kravet om "privacy by design".
- ☐ Utveckla rutiner för hur ni ska göra då ni samarbetar med andra, eftersom varje led i kedjan kommer att hållas individuellt ansvarigt för hanteringen av personuppgifter.
- ☐ Upprätta en process för att kunna informera Datainspektionen samt berörd person inom 72 timmar vid en personuppgiftsincident.

Ta reda på mer

I den här broschyren har vi samlat huvuddragen i den nya dataskyddsförordningen (GDPR). För mer information besöker du Datainspektionens hemsida **www.datainspektionen.se**. Där har du också möjlighet att ställa frågor.

BRANDLINE NOVEMBER 2017

SoftOne®
www.softone.se

STOCKHOLM
Klarabergsgatan 23
Box 596
101 31 Stockholm
0771-55 69 00
marknad@softone.se

GÖTEBORG
Gårdatorget 1, 4 tr.
412 50 Göteborg
0771-55 69 00
marknad@softone.se

HELSINGFORS
Perintötie 2 b
01510 Vantaa
+358 9 3507 750
myynti@softone.fi