EVERSHEDS SUTHERLAND

De rätta stegen

Hur ni säkerställer att er verksamhet är i förenlighet med GDPR

GDPR kräver ett nytt synsätt på integritet och skydd av personuppgifter samt användande av desamma. Verksamheter måste planera för integritetsfrågor och införliva principen om dataminimering i sina affärsprocesser.

Sanktioner:
Organisationer som inte uppfyller kraven enligt GDPR kan drabbas av vite på upp till det högsta av 4% av den globala årsomsättningen eller 20 miljoner euro!

1 Tillsätt en projektgrupp

Om ni inte redan har gjort det, bör ni:

- tillsätta en projektgrupp och fördela ansvaret för att driva organisationens GDPR-projektet framåt
- bestäm om er strategi och ert GDPR-projekt ska drivas på koncernnivå eller inom enskilda operativa bolag
- säkra styrelsens godkännande av de resurser som är nödvändiga för att genomföra ert GDPR-projekt
- bestäm vilken av era enheter inom EU som utgör ert huvudsakliga verksamhetsställe

2 Dataskyddsombud

Överväg om ni ska utse ett dataskyddsombud. Ett dataskyddsombud måste utses av:

- myndigheter
- privata aktörer vars kärnverksamhet i stor utsträckning omfattar behandling av känsliga personuppgifter eller särskilda kategorier av personuppgifter, eller omfattar systematisk och regelbunden kartläggning av registrerade

3 Uppdatera policys och dokumentation avseende integritet

- uppdatera befintliga policys och skapa nya policys för att reglera de brister som uppmärksammats i GAP-analysen
- detta kommer att omfatta ex. integritetspolicys, formulering av samtycke, gallringspolicys, policy för hantering av registrerads begäran om tillgång till information, policys avseende behandling av personuppgifter

4 Kartlägg personuppgiftsbehandling

- förstå och kartlägg er behandling av personuppgifter
- skapa tydlig dokumentation av den behandling av personuppgifter som sker under ert ansvar
- uppdatera er genomförandeplan efter att ha verifierat den mot kartläggningen av behandling av personuppgifter

5 GAP-analys

- analysera alla policys, rutiner och behandling av personuppgifter utifrån de krav som ställs enligt GDPR
- ta organisationens riskaptit avseende personuppgiftsfrågor och förenlighet med lag i beaktande
- sammanställ en rapport för ledningen i vilken de brister som uppmärksammats i analysen redogörs för tillsammans med förslag till åtgärder (omfattande även information om förväntat behov av resurser, tidsplan och föreslagen prioriteringsordning)
- prioritera de områden som medför högst risk vid implementering av föreslagna lösningar
- ta vägledningar och riktlinjer från Datainspektionen och Artikel 29 Arbetsgruppen i beaktande i takt med att de görs tillgängliga

6 Inför rutiner

- säkerställ att "privacy by design" och konsekvensanalyser införs som standard och att mallar finns i den utsträckning det är möjligt
- uppdatera rutiner avseende hantering av registrerades rättigheter (ex. rätt till information, dataportabilitet, rättelse och invändning mot behandling)

7 Uppdrag till tredje man

- granska era leverantörer och omförhandla avtal för att säkerställa att avtalen uppfyller de krav som GDPR ställer och att nödvändiga villkor för personuppgiftsbiträden omfattas på lämpligt vis
- säkerställ att alla nya leverantörer utses på GDPR-förenliga villkor
- se över hur ni genomför granskning av leverantörer och förbered lämpliga kravlistor och underlag för att dokumentera sådan kontroll
- bedöm eventuell påverkan av GDPR på övriga villkor i era avtal, exempelvis avseende ansvar

8 Utbildning

- utbilda beslutsfattare och projektgrupper innan projektet påbörjas
- säkerställ att all personal genomför lämplig utbildning för deras respektive ansvarsområden innan den 25 maj 2018

För mer information, kontakta:

Richard Jacobsson
Partner

richardjacobsson@eversheds-sutherland.se

Josefine Karlsson
Associate

josefinekarlsson@eversheds-sutherland.se

Viktiga begrepp

Några begrepp som är nödvändiga att förstå

Kärnbegrepp

Territoriell omfattning: GDPR äger tillämpning för organisationer som:

- behandlar personuppgifter i egenskap av personuppgiftsansvarig eller personuppgiftsbiträde inom EU (oaktat om behandlingen genomförs inom EU)
- behandlar personuppgifter i egenskap av personuppgiftsansvarig inom EU även om själva behandlingen genomförs utanför EU
- behandlar personuppgifter i egenskap av personuppgiftsbiträde på uppdrag en personuppgiftsansvarig som lyder under GDPR även om organisationen är belägen utanför EU eller om behandlingen sker utanför EU
- som inte är etablerade inom EU men som behandlar personuppgifter om registrerade som befinner sig inom EU i anknytning till: (a) tillhandahållande av varor eller tjänster till dem, oavsett om de erlägger betalning eller ej, eller (b) om registrerades beteenden inom EU bevakas

One stop shop: En organisation som har mer än ett verksamhetsställe inom EU kan ha möjlighet att helt eller delvis ha att göra med enbart en tillsynsmyndighet såsom dess huvudsakliga tillsynsmyndighet avseende gränsöverskridande behandling av personuppgifter som genomförs inom organisationen.

Ansvar: En personuppgiftsansvarig ansvarar för och måste kunna visa förenlighet med principerna för behandling av personuppgifter.

Samtycke: Ett samtycke måste vara en frivilligt, specifikt, informerat och lämnas genom ett uttalande eller en entydig bekräftande handling som leder till en överenskommelse om behandling av individens personuppgifter. Underförstått samtycke eller förifyllda boxar är inte tillräckligt.

Uppgiftsminimering: Personuppgifter ska vara adekvata, relevanta och begränsade till de uppgifter som är nödvändiga för ändamålen med behandlingen.

Skyldigheter för personuppgiftsbiträden: Av GDPR följer skyldigheter för personuppgiftsbiträden när de behandlar personuppgifter på uppdrag av personuppgiftsansvariga. Sådana skyldigheter avser exempelvis säkerhetsåtgärder, internationell överföring av personuppgifter, utseende av underbiträden och notifiering av personuppgiftsincidenter.

Internationell överföring av personuppgifter: GDPR kodifierar nya adekvata säkerhetsåtgärder för överföring av personuppgifter utanför EU, vilka omfattar:

- bindande företagsbestämmelser
- standardavtalsklausuler som godkänts av den lokala tillsynsmyndigheten
- godkända uppförandekoder
- godkända certifieringsmekanismer

Registrerades rättigheter

Registrerads rätt att begära information: Registrerade har rätt att begära mer omfattande information, ex. detaljer om:

- de säkerhetsåtgärder som personuppgiftsansvarig har vidtagit för internationell överföring av personuppgifter
- den period under vilken personuppgiftsansvarig avser lagra den registrerades personuppgifter

I de flesta fall ska informationen som en registrerad begär tillhandahållas utan oskäligt dröjsmål och i vart fall inom en månad efter mottagandet av begäran. Om det inte är uppenbart ogrundat eller orimligt måste informationen tillhandahållas utan kostnad.

Radering: Personuppgifter måste raderas utan oskäligt dröjsmål om:

- behandling av personuppgifterna inte längre är nödvändig
- samtycket dras tillbaka och det inte finns någon annan legal grund för behandlingen
- den registrerade invänder mot behandlingen och det saknas berättigade skäl som väger tyngre än den registrerades intressen
- personuppgifterna har behandlats olagligt
- radering krävs för att uppfylla en rättslig skyldighet

Portabilitet: Om personuppgifter har tillhandahållits av den registrerade och behandlingen sker automatiserat baserat på ett samtycke eller om behandlingen är nödvändig för att uppfylla ett avtal med den registrerade måste den personuppgiftsansvarige tillhandahålla de relevanta personuppgifterna till den registrerade eller till en personuppgiftsansvarig utpekad av den registrerade om den registrerade begär det. Uppgifterna ska tillhandahållas i ett strukturerat, allmänt använt och maskinläsbart format.

Profilering och automatiserade beslut: Registrerade har rätt att inte bli föremål för beslut som enbart grundas på någon form av automatiserat beslutsfattande, inbegripet profilering, om beslutet kan ha rättsliga följder för den registrerade eller på liknande sätt i betydande grad påverkar denne (ex. automatiserat beslut på en kreditansökan eller nekande besked från e-rekrytering via internet utan personlig kontakt).

Rättning: Registrerade har rätt att begära att en personuppgiftsansvarig utan oskäligt dröjsmål rättar dennes personuppgifter om de är oriktiga.

Begränsning av behandling: Registrerade har rätt att kräva att behandlingen av personuppgifter begränsas om:

- den registrerade bestrider personuppgifternas korrekthet, under en tid som ger den personuppgiftsansvarige möjlighet att kontrollera om personuppgifterna är korrekta
- behandlingen är olaglig och individen kräver att behandlingen begränsas i stället för att uppgifterna raderas
- personuppgiftsansvarig inte längre behöver uppgifterna för ändamålen med behandlingen men den registrerade behöver dem i relation till rättsliga anspråk
- den registrerade har invänt mot behandlingen i enlighet med dennes rättighet att göra så (och begränsningen ska då gälla i väntan på kontroll av huruvida den personuppgiftsansvariges berättigade skäl väger tyngre än den registrerades berättigade skäl

Rätt att göra invändningar: Registrerade har, baserat på dennes specifika situation, rätt att invända mot behandling av personuppgifter vilken baseras på allmänt intresse eller en intresseavvägning.

Krav på system och rutiner

Privacy by design: En personuppgiftsansvarig måste vid den tid medlen för behandling av personuppgifter bestäms och vid tiden för genomförande av behandlingen implementera lämpliga tekniska och organisatoriska åtgärder vilka är utformade för att:

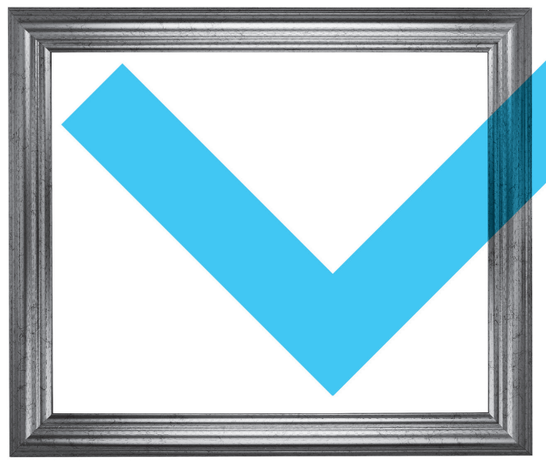
- implementera principer för personuppgiftsbehandling (ex. uppgiftsminimering)
- integrera nödvändiga säkerhetsåtgärder för att uppnå de krav som ställs enligt GDPR och för att skydda de registrerades rättigheter

Utseende av personuppgiftsbiträden: Personuppgiftsansvarig får bara utse personuppgiftsbiträden som ställer tillräckliga garantier för att behandlingen kommer att uppfylla de krav som ställs enligt GDPR och all behandling måste regleras i ett avtal eller annan bindande handling vilken omfattar de i GDPR angivna skyldigheterna för personuppgiftsbiträden. Personuppgiftsbiträden har inte heller rätt att utse andra personuppgiftsbiträden (ex. ett underbiträde) utan den personuppgiftsansvariges samtycke och måste i vissa fall tillse att motsvarande avtalsklausuler som de mellan den personuppgiftsansvarige och personuppgiftsbiträdet gäller även mellan personuppgiftsbiträdet och underbiträdet.

Rapportering av personuppgiftsincidenter: Organisationer ska rapportera en personuppgiftsincident enligt följande:

- personuppgiftsansvarige: (a) till tillsynsmyndigheten utan oskäligt dröjsmål men senast inom 72 timmar efter att incidenten kom till dess vetskap, och (b) till registrerade utan oskäligt dröjsmål, om incidenten sannolikt kan leda till hög risk för individen
- personuppgiftsbiträde, till den personuppgiftsansvarige utan oskäligt dröjsmål efter att incidenten kom till dess vetskap

Konsekvensbedömning: En konsekvensbedömning måste genomföras om en form av behandling (i synnerhet vid användande av ny teknik) sannolikt kommer att leda till hög risk för individers rättigheter och friheter.



eversheds-sutherland.com

DTUK001694_06/18