GLOBAL BUSINESS TRAVEL

Dataskyddsförordningen (GDPR): är du redo?

American Express Global Business Travel April 2018

Hur du förbereder ditt reseprogram så att det är redo för ändringar i dataskyddslagen

Introduktion

När Europeiska unionens Dataskyddsförordning (GDPR) träder i kraft den 25 maj 2018 innebär det den mest omfattande uppdateringen av globalt dataskydd på flera decennier.

Målet med GDPR är att säkerställa att företag är tydliga med och ansvariga för hur de hanterar personuppgifter. Förordningen täcker alla delar av verksamheten, och gör det möjligt att vidta stränga sanktioner, inklusive böter på upp till 20 miljoner Euro eller 4 % av den globala omsättningen, beroende på vilken summa som är högst.

Företag som är förpliktigade att följa den nya förordningen kommer att behöva ha strikta rutiner för hur de samlar in, lagrar och använder personuppgifter i sin verksamhet. Det innebär att företagen måste ha en tydlig förståelse för var personuppgifterna som behandlas finns, hur de används och hur uppgifterna skyddas.

Världsomspännande påverkan

En betydande förändring i förhållande till tidigare personuppgiftslag är omfattningen av GDPR:s extraterritoriella tillämpningsområde: Trots att reglerna har utformats av Europeiska unionen (EU) kommer troligtvis även företag i andra länder behöva uppfylla kraven i GDPR om de har en närvaro, erbjuder varor och tjänster eller övervakar personers beteende inom EU.

Forskning tyder på att få företag är redo för det nya regelverket. Enligt *2017 Veritas GDPR Report* var 86 % av 900 undersökta företag runt om i världen oroade över att en underlåtelse att följa GDPR kan ha en stor negativ påverkan på deras verksamhet.

INBYGGT DATASKYDD:

American Express Global Business Travel (GBT) är redo för GDPR

Vårt arv som del av ett holdingbolag inom bankväsendet och våra rötter inom finansiell regelefterlevnad och säkerhet har gjort oss väl rustade för att uppfylla GDPR:s ansvarskrav. Sedan 2015 har American Express GBT skapat, genomfört och förbättrat programmet för hantering av integritetsrisker (Privacy Risk Management Programme), ett ansvarsramverk som utvecklats med beredskap för GDPR i åtanke.

Programmet för hantering av integritetsrisker fungerar sömlöst med American Express GBT:s datahanteringsprogram och ett ramverk för hantering av säkerhetsrisker. Tillsammans hjälper dessa samverkande program till att säkerställa en djupgående regelefterlevnad, inkluderade:

- ansvarig personal inom dataskydd, inklusive ett dataskyddsombud
- utbildning inom integritetsskydd för företag samt inom säkerhetsmedvetenhet
- påvisbar undersökning och rapportering gällande integritetsskydd och regelefterlevnad inom säkerhet
- regelbundna interna revisioner
- uppdaterade integritetspolicys
- omfattande riskhantering avseende ansvar som personuppgiftsbiträde, inklusive biträdesavtal samt regelbunden integritets- och säkerhetsriskbedömning

Dataskyddslagstiftningen handlar om två sammanvävda koncept:

- Vilka rättigheter har individen vad gäller dennes personuppgifter?
- Vilka rutiner behöver företag införa för att garantera att dessa rättigheter respekteras?

FOKUS PÅ INDIVIDEN

Enligt GDPR har individer rätt att få veta vilka personuppgifter som ett företag har om dem. Dessa individer benämns enligt GDPR för "registrerade". Företag måste underrätta registrerade om varför företaget samlar in deras personuppgifter och avslöja sådana uppgifter om deras datafunktioner som säkerställer att de agerar med öppenhet.

Registrerade har även rätt att bestämma hur deras uppgifter används. Företag måste, under vissa förutsättningar, möjliggöra för registrerade att godkänna/neka behandling, radera uppgifter eller överföra sin data till en ny leverantör - detta kallas för deras "rätt till dataportabilitet".

För att uppfylla kraven i GDPR är det inledningsvis viktigt att förstå vad personuppgifter är. Det inkluderar information som traditionellt anses vara personuppgifter, såsom namn, passnummer och födelsedatum. Men GDPR klargör och bekräftar att begreppet även omfattar annan information som gör att företag kan identifiera, lokalisera, kontakta eller peka ut en individ, inklusive genom unika identifierare som exempelvis IP-adresser eller mobiltelefonidentifierare - samt den typ av reseuppgifter och sökare som dominerar inom resetjänster.

Hur du förbereder ditt GDPR-kompatibla integritetskyddsprogram

Personuppgiftsbestämmelser har alltid krävt att företag har policys och supportsystem på plats som skyddar personliga uppgifter och säkerställer att registrerade kan få tillgång till uppgifterna. Den största skillnaden som följer av GDPR i det här avseendet är ansvarsskyldigheten. Det är inte längre tillräckligt att bara följa lagen, företag måste även kunna visa att de följer den.

När du förbereder arbetet med att bli kompatibel med GDPR, fokusera då på att utveckla ett stabilt ramverk för ansvarsskyldigheten som gör att du kan dokumentera, mäta och kommunicera dina personuppgiftsbehandlingar. Byggstenarna för att göra detta är bland andra:

SKAPA EN UPPGIFTSFÖRTECKNING

Vissa personuppgifterslagar har tidigare inkluderat ett koncept som kallas för "register över behandling", som innebar krav för företag att upprätthålla en skriftlig rapport med information om all sin personuppgiftsbehandling. GDPR inför det här kravet för samtliga reglerade företag.

"Det verkar självklart, men det första steget i att säkerställa att all personuppgiftsbehandling görs enligt gällande rätt är att kartlägga vilka uppgifter du har, var de finns och varför du har dem," säger Kasey Chappelle, Chief Privacy Officer på American Express GBT. "Det är inte bara gällande rätt - smarta företag kommer att se detta som en möjlighet att bygga upp en uppgiftsförteckning som är avgörande för en god datahantering."

TRANSPARENT PERSONUPPGIFTSBEHANDLING

Företag måste säkerställa att de kommunicerar sin personuppgiftsbehandling på ett effektivt och öppet sätt till de registrerade. Det innebär bland annat att ha en fullständig och regelrätt personuppgiftspolicy. "Ett företags personuppgiftspolicy måste vara lättläst: koncis, tydlig och skriven på ett rakt och enkelt språk, samt vara lättillgänglig - så att alla kan förstå hur deras personuppgifter kommer att användas och kunna ge meningsfullt samtycke där det behövs," säger Chappelle.

Personuppgiftspolicyn måste även beskriva hur personuppgifter kan överföras inom verksamheten, till tredje part och andra jurisdiktioner, samt hur registrerade kan utöva sina rättigheter.

Transparens består inte bara av en personuppgiftspolicy. Företag kan se till att registrerade förstår hur deras personuppgifter används genom att i deras varor och tjänster bygga in skydd för den personliga integriteten (privacy by design) — ett koncept som nu även ingår som krav i GDPR:s nya skyldigheter vad gäller inbyggt integritetsskydd som standard.

REGELRÄTTA INTERNATIONELLA ÖVERFÖRINGAR

Företag måste förstå de strikta krav som följer av lagen gällande internationella överföringar, i synnerhet för tjänster såsom resor som till sin natur är gränsöverskridande. Uppgifter inom EU måste fortsättningsvis skyddas enligt en europeisk standard överallt där de lagras, nås eller behandlas, oavsett var i världen det sker, både inom företagsfamiljen och när de delas med tredjepartsbehandlare.

Företag kan uppnå överensstämmelse med GDPR på flera sätt, till exempel genom att anta EU-godkända bindande företagsinterna regler eller genom att underteckna en uppsättning av EU:s standardavtalsklausuler. Först och främst är det viktigt att företag förstår sina dataflöden, och därefter kan de säkerställa att det finns lämpliga rutiner på plats för var och en.

EFFEKTIV HANTERING AV DATASKYDDSRISKER INOM LEVERANSKEDJAN

Det är viktigt för företag att ha förtroende för att andra företag till vilka de överför personuppgifter även uppfyller globala regler avseende integritetsskydd.

Resetjänster innebär enormt komplexa dataöverföringar. Varje dag överförs personuppgifter som t.ex. namn och passnummer från registrerade till en rad olika tredje parter. Om denna information inte hade kunnat överföras, hade resor varit omöjliga.

En del av de många företag som tar emot resedata, som t.ex. globala distributionssystem, flygbolag, hotell och andra reseleverantörer, identifieras av EU:s ansvariga tillsynsmyndigheter som personuppgiftsansvariga vilka lyder direkt under dataskyddslagen. Andra är personuppgiftsbiträden — företag som endast hanterar data på uppdrag av en annan personuppgiftsansvarig.

I och med GDPR skärps reglerna för hur en personuppgiftsansvarig anlitar och har tillsyn över ett personuppgiftsbiträde, och det införs nya direkta regler även för personuppgiftsbiträden. Företag kommer endast att kunna leva upp till kraven i GDPR om de har fasta rutiner för hantering av tredjepartsrelationer.

American Express GBT har ett nära samarbete med tredjepartsleverantörer för att utvärdera hur de hanterar personuppgifter samt säkerställa att de förstår och möter kraven.
"Personer som köper resor och samarbetar med resebyråer vill bli försäkrade om att resebyrån inte bara har integrerat data- och integritetsskydd i sina processer, utan även i processerna för rekrytering av nya leverantörer," säger Chappelle. "Här på American Express GBT innebär denna process samma integritetsbedömning som vi använder för vår egen produktutveckling — leverantörer måste kunna visa att de har lämpliga rutiner för integritetsskydd och rätt säkerhetsprotokoll på plats."

UTSE ETT DATASKYDDSOMBUD

För att kunna följa GDPR kommer många företag behöva utse ett dataskyddsombud — en anställd på företaget som ska ansvara för företagets efterlevnad av dataskyddsreglerna, och måste ha rätt stöd, resurser, verktyg, kunskap och behörighet för att kunna utföra arbetet på ett effektivt sätt. En del företag kommer att kunna outsourca ansvaret till en behörig extern expert.

EFFEKTIV PRIORITERING AV DATAINTRÅNG

Obligatoriska meddelanden avseende överträdelser är en stor del av EU:s integritetsregler. Enligt GDPR finns det två underrättelsekrav om en individs personuppgifter har komprometterats. Det aktuella landets datatillsynsmyndighet måste underrättas inom 72 timmar efter att överträdelsen har blivit känd. I en del fall måste även den registrerade underrättas.

Prioritering är en process där man kategoriserar frågor och delar in dem i prioritetsnivåer — i det här avseendet potentiella och verkliga överträdelser av integritetsskyddsbestämmelser. Att utveckla ett prioritetsbaserat system för hantering av klagomål och andra frågor gör det möjligt för företagen att identifiera och prioritera potentiella överträdelser av integritetsskydd och säkerhet. De måste kunna prioritera bland klagomål och rapporter, snabbt kunna identifiera, tilldela och åtgärda en överträdelse, samt ha rutiner på plats för att kommunicera med tillsynsmyndigheter och påverkade individer.

”På American Express GBT har vi en flerskiktad strategi för att identifiera problem och hantera klagomål som gäller integritetsskydd eller säkerhet”, säger Chappelle. "En telefon- och webbaserad hotline är tillgänglig dygnet runt för alla anställda, där de kan prata med något på valfritt språk. Alla klagomål från anställda kategoriseras omedelbart — t.ex. som dataskydd, säkerhets- eller personalfråga, och kan därefter tilldelas till rätt avdelning."

SLUTSATS

GDPR är en möjlighet för organisationer och deras leverantörer att tillsammans skapa en ömsesidig förståelse för dessa nya skyldigheter, och se till att de system och processer som existerar mellan företagen är förenliga med de nya reglerna. Detta arbete bör även inkludera utveckling av system och tillvägagångssätt som ska följas vid regelbrott.

Tanken är att se dataskydd som ett spörsmål för hela verksamheten, att ha ett nära samarbete med tredje parter och leverantörer, samt att integrera dataskydd i den dagliga verksamheten.

Kom ihåg: deadline för GDPR är den 25 maj 2018.

Om ditt företag ännu inte har tagit upp dessa frågor är det dags att göra det nu. Även om dina reseleverantörer är "personuppgiftsansvariga" är även du det när det gäller ansvaret för dina anställdas personuppgifter.

Ett av dina första steg i arbetet bör vara att prata med din resebyrå och fråga om de har implementerat de bästa rutinerna för att vara redo för att efterleva GDPR.

GLOBAL BUSINESS TRAVEL

VILL DU VETA MER?

Kontakta American Express GBT på:

https://www.amexglobalbusinesstravel.com/se/contact/

E-post: nordicsales@amexgbt.com