COMPLIANCE PARTNERS

Nyckelinsikter

GDPR-EFTERLEVNAD:

VAD DU BÖR TÄNKA PÅ INNAN DU ÖVERÖR PERSONUPPGIFTER GLOBALT

Innehållsförteckning

Introduktion till GDPR och Tredjelandsöverföringar

GDPR (General Data Protection Regulation) är utformad för att skydda individers personuppgifter inom EU och säkerställa att företag behandlar dessa uppgifter på ett transparent och lagligt sätt. Vid internationella överföringar, särskilt till länder utanför EU/EES, måste företag vidta extra försiktighetsåtgärder för att säkerställa att den skyddsnivå som GDPR kräver bibehålls.

Tredjelandsöverföringar är särskilt relevanta för företag som arbetar med globala partners, leverantörer eller tjänster som finns utanför EU/EES området. Det kan vara en juridisk och teknisk utmaning att säkerställa att överföringar sker på ett säkert sätt.

Nyckelprinciper för Tredjelandsöverföringar inom GDPR

Adekvat skyddsnivå:

- EU-kommissionen bedömer om ett tredjeland erbjuder tillräcklig skyddsnivå för personuppgifter.
- Länder med adekvat skyddsnivå inkluderar Andorra, Argentina, Japan, och Storbritannien.

Schrems-domen:

- Denna dom underkände Privacy Shield-avtalet mellan EU och USA, vilket tvingar företag att använda alternativa mekanismer som SCCs för att överföra data lagligt.

Överföringsmekanismer:

- Alternativ som Standardavtalsklausuler (SCCs) och Binding Corporate Rules (BCRs) används för att säkerställa att data överförs på ett lagligt och säkert sätt.

Begreppsordlista

SCCs (Standardavtalsklausuler): Standardavtalsklausuler som godkänts av EU för att möjliggöra lagliga överföringar av personuppgifter till tredjeländer.
Binding Corporate Rules (BCRs): Interna regler för multinationella företag som tillåter överföring av data inom samma företagsgrupp, även utanför EU.
Transfer Impact Assessment (TIA): En riskbedömning som genomförs när personuppgifter överförs till tredjeländer för att säkerställa att dataskyddslagar följs.
Schrems II: En viktig dom som ogiltigförklarade Privacy Shield-avtalet mellan EU och USA, vilket förändrade hur dataöverföringar mellan dessa länder regleras.
Pseudonymisering: En metod för att minska riskerna vid databehandling genom att ersätta identifierande information med konstgjorda data.

Överföring av Personuppgifter: Schrems, SCCs och TIA

Schrems I och II: Påverkan på Överföringar

- Schrems I: EU-domstolen ogiltigförklarade Safe Harbor-avtalet eftersom det inte säkerställde tillräckligt skydd för europeiska personuppgifter.
- Schrems II: Domstolen ogiltigförklarade Privacy Shield-avtalet och krävde att alla överföringar till USA måste vara förenliga med GDPR, vilket gjorde att Standardavtalsklausuler (SCCs) blev en nödvändig mekanism.

Överföringsmekanismer:

Om ett beslut om adekvat skyddsnivå saknas, kan företag använda andra mekanismer som:

- Standardavtalsklausuler (SCCs): Godkända av EU-kommissionen och används för att överföra data på ett säkert sätt.
- Binding Corporate Rules (BCRs): Interna dataskyddspolicys för företag.

Vad är nytt med de uppdaterade SCCs?

År 2021 uppdaterade EU-kommissionen SCCs för att förbättra transparens, rättigheter och incidenthantering. Kommande förändringar väntas under 2025.

Transfer Impact Assessment (TIA):

- En TIA bör utföras för att bedöma riskerna vid överföring av data till tredjeland och för att säkerställa att lämpliga skyddsåtgärder vidtas.
- TIA måste innehålla en bedömning av mottagarlandets lagar, rättssäkerhet, och om det finns en oberoende tillsynsmyndighet.

Framgång och Misslyckanden: Case Studies

Framgång

- Ett medelstort teknikföretag implementerade SCCs korrekt och genomförde TIA-rapporter, vilket skyddade dem från böter och upprätthöll kundernas förtroende.

Misslyckande

- Uber, ett globalt transportföretag, bötfälldes med 3,3 miljarder kronor av den nederländska dataskyddsmyndigheten för att ha överfört känsliga personuppgifter till USA utan tillräckligt skydd. Följande personuppgifter överfördes under mer än två år:
  - Kontouppgifter, taxilicenser, platsdata, foton, betalningsuppgifter, identitetshandlingar, brottsregister och sjukjournaler.

  Uber hade initialt använt sig av SCCs men slutade göra det 2021 utan att implementera nya överföringsmekanismer. Dataintrång upptäcktes, vilket ledde till att hackare fick tillgång till dessa uppgifter. Uber misslyckades även med att informera berörda parter och genomföra nödvändiga Transfer Impact Assessments (TIA).

  Detta fall belyser vikten av att:

  1. **Upprätthålla aktuella överföringsmekanismer.**
  2. **Genomföra konsekvensbedömningar (TIA).**
  3. **Implementera tekniska och organisatoriska skyddsåtgärder**, såsom kryptering och pseudonymisering.
  4. **Rapportera incidenter i tid.**

Hur man Undviker GDPR-böter och Säkerställer Efterlevnad

- **Tydliga interna rutiner:** Företag bör ha rutiner för hantering av personuppgifter.
- **Konsekvensbedömningar (TIA):** Utför TIA vid varje tredjelandsöverföring.
- **Dokumentation:** Dokumentera alla överföringar noggrant.
- **Övervakning och revision:** Intern och extern revision för att upptäcka brister i efterlevnaden.

Verktyg och Tekniker för GDPR-Efterlevnad

- **Data Mapping Tools:** Kartlägg dataflöden och lagringsplatser.
- **Kryptering och Pseudonymisering:** Använd kryptering för att skydda data.
- **Säkerhetscertifieringar:** Exempelvis ISO 27001 och SOC 2-certifieringar.
- **GDPR Scanners:** Identifiera risker och säkerställ efterlevnad.

Framtiden för GDPR och Internationella Dataöverföringar

Företag bör hålla sig uppdaterade om nya domar och lagändringar, särskilt de som påverkar tredjelandsöverföringar, som USAs roll i det nuvarande EU-U.S. Data Privacy Framework. Regelbundna förändringar i lagstiftningen, såsom uppdateringar av Schrems-domen eller förändringar i överföringsmekanismer, kan få stor påverkan på företagets dataskyddsstrategi.

Därför är det avgörande att företag inte bara anpassar sina processer utan också regelbundet genomför intern revision och utbildar sina medarbetare för att säkerställa att de snabbt kan reagera på nya juridiska krav och undvika eventuella GDPR-böter.