Elavon

Efterlevnads-förberedelse

En handledning
till den allmänna
dataskyddsförordningen
(GDPR)

elavon.se

Den allmänna dataskyddsförordningen (GDPR) kommer att reglera integriteten och hanteringen av personuppgifter för de privatpersoner som bor inom Europeiska unionen (EU). Den här handledningen förklarar vad den innebär, hur den påverkar privatpersoner och verksamheter som din och ger dig all information du behöver om den nya förordningen.

Sammanfattning av GDPR

När träder den nya förordningen i kraft?

25 maj 2018

Vad är det som är nytt med den här förordningen?

Privatpersoner har fått nya rättigheter som rör åtkomst till de uppgifter som företag har om dem och den omfattar även förpliktelser för bättre datahantering av företagen och nya bötesstraff.

Vad är GDPR?

I januari 2012 fastställde Europeiska kommissionen en plan för en dataskyddsreform för hela den Europeiska unionen, för att ”anpassa Europa till den digitala eran”. Nästan fyra år senare, uppnåddes ett avtal om vad den skulle inkludera och hur den skulle verkställas.

En av huvudpunkterna i reformen var introduktionen av den allmänna dataskyddsförordningen. Det här nya regelverket för EU gäller för alla organisationer i alla medlemsstater och för globala verksamheter som gör affärer med privatpersoner inom EU.

GDPR är i stort sett en uppsättning av nya regler som ger privatpersoner större kontroll över sina uppgifter. Den strävar efter att förenkla den regulatoriska miljön för företag så att både privatpersoner och företag kan nyttja den digitala ekonomin fullt ut.

Reformen har utformats för att återspegla världen vi lever i nu och den uppdaterar lagar och förpliktelser i Europa för att följa de villkor som finns i den internetanslutna eran.

I grund och botten, kretsar alla aspekter av våra liv runt data.
Det gäller allt från sociala medie-företag, till banker, återförsäljare och statliga myndigheter, och nästan alla tjänster vi använder inkluderar insamling och analys av våra personuppgifter. Ditt namn, din adress, ditt betalkortsnummer och mer samlas in, analyseras och, kanske allra viktigast, lagras av olika organisationer. GDPR har som mål att harmonisera regelverken i Europa så att de återspeglar dagens miljö av datautbyte.

Vad innebär det för min organisation?

GDPR kommer att gälla för organisationer eller privatpersoner som hanterar någon typ av personuppgifter för personer bosatta inom EU. Det innebär att företag och privatpersoner som är baserade utanför EU som säljer varor och tjänster till privatpersoner bosatta inom EU även måste efterleva den nya lagen. Det sista innebär att nästan alla stora bolag i världen måste vara förberedda på vad GDPR innebär när den börjar gälla och börja arbeta på en strategi för GDPR-efterlevnad. GDPR gäller för personuppgiftsansvariga, gemensamt personuppgiftsansvariga och för personuppgiftsbiträden, men det är viktigt att känna till skyldigheterna för de olika rollerna.

Är du en personuppgiftsansvarig eller ett personuppgiftsbiträde?

De olika termerna

De som hanterar privatpersonernas uppgifter har inte samma roll och dataskyddslagar tillåter hanteringen genom tre olika kategorier: Personuppgiftsansvarig, gemensamt personuppgiftsansvariga och personuppgiftsbiträde. Det innebär:

Personuppgiftsansvarig

En personuppgiftsansvarig är en entitet (privatperson eller företag) som fastställer ändamålen och medlen för behandlingen av personuppgifterna.

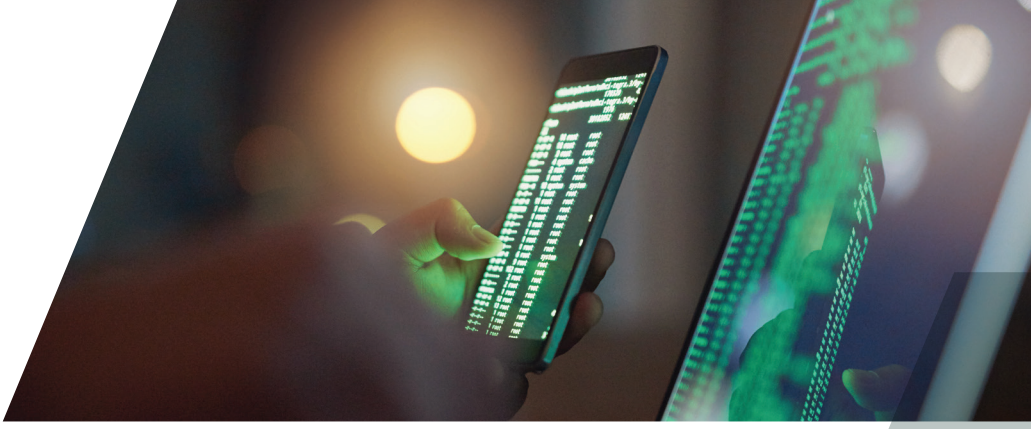
Gemensamt personuppgiftsansvariga

När två eller fler företag tillsammans fastställer ändamålen och medlen för behandlingen av personuppgifterna. De bestämmer exempelvis tillsammans ändamålen/orsakerna bakom, tillfälle, typ, omfattning och mål med behandlingen.

Personuppgiftsbiträde

Personen eller gruppen som behandlar personuppgifter på den personuppgiftsansvariges vägnar. Behandling är att samla in, registrera, anpassa eller lagra personuppgifter.

Samma entitet kan både vara personuppgiftsansvarig och personuppgiftsbiträde, beroende på omständigheterna. Om till exempel ett teknikföretag tillhandahåller betalningsbehandlingsteknologi till handlare online är teknikföretaget personuppgiftsbiträdet och handlaren den personuppgiftsansvarige. Men om teknikföretaget paketerar samma personuppgifter för att tillhandahålla målinriktade kundsegment till annonsörer, agerar det som en personuppgiftsansvarig.



GDPR ställer slutligen rättsliga krav på den personuppgiftsansvarige, för hur man ska lagra personuppgifter och hur de ska behandlas, genom att ange ett betydligt högre rättsligt ansvar om organisationen skulle utsättas för intrång.

Den personuppgiftsansvarige måste även se till att alla avtal med personuppgiftsbiträden följer GDPR:s krav.

Vad är personuppgifter och känsliga personuppgifter?

Under den befintliga lagstiftningen anses personuppgifter inkludera namn, adress och foton. GDPR utökar definitionen av personuppgifter så att de i vissa fall även kan inkludera exempelvis en IP-adress. Den inkluderar även känsliga personuppgifter såsom genetiska och biometriska uppgifter, som skulle kunna behandlas för att unikt identifiera en privatperson.

Personuppgifter

Uppgifter relaterade till en levande person som kan identifieras direkt eller indirekt, t.ex. via:

- Namn
- Telefonnummer
- E-postadress
- Betalkortsnummer

Känsliga personuppgifter

Personuppgifter som består av uppgifter såsom:

- Den registrerades ras eller etniska ursprung
- Politiska åsikter
- Religiösa eller andra trosuppfattningar av liknande typ
- Eventuellt fackföreningsmedlemskap
- Fysisk(t) eller psykisk(t) hälsa eller tillstånd
- Sexliv

Vad anger GDPR?

Det finns 99 artiklar inom GDPR. De går från allmänna bestämmelser, den personuppgiftsansvariges, de gemensamt personuppgiftsansvarigas och personuppgiftsbiträdets ansvar, till skyldigheten att samarbeta med tillsynsmyndigheter.

Viktiga förändringar som kan påverka din organisation inkluderar:

- **Inbyggt dataskydd** – Dataskyddet måste byggas in i företagsprocesser och system redan från start och tillhandahållas som standard.
- **Rätt att bli bortglömd** – Användare kan begära att få sina uppgifter raderade. De kan även begära att få en kopia av uppgifterna skickade till en tredje part.
- **Obligatorisk underrättelse om incidenter** – Vissa personuppgiftsincidenter måste nu rapporteras till myndigheterna inom 72 timmar och till berörda personer utan dröjsmål.
- **Straff för de som inte efterlever kraven** – GDPR tillåter böter på upp till 20 miljoner euro eller 4 procent av företagets årliga omsättning, beroende på vad som är högst.

Hur ser GDPR-efterlevnad ut?

Det finns inget enskilt koncept för hur man ska förbereda sig för GDPR.

Varje enskilt företag måste fastställa exakt vad det behöver göra för att efterleva dataskyddsförordningen. Det är viktigt att förstå om du är personuppgiftsansvarig eller personuppgiftsbiträde. De flesta företag kommer troligtvis att vara både personuppgiftsansvarig och personuppgiftsbiträde, beroende på de specifika uppgifter det tar emot.

Hur man förbereder sig

- Börja med att få en förståelse för vilka personuppgifter som företaget innehar och vilka som har åtkomst till dem
- Begränsa åtkomsten baserat på affärsbehov och implementera övervakning för att upptäcka eventuell obehörig åtkomst
- Gör en bedömning om vilka efterlevnads- och säkerhetskontroller du har på plats för att samla in och skydda uppgifterna, hur effektiva de är och var behoven finns
- Utveckla en plan för att förbättra ditt säkerhetsprogram, genom att titta på medarbetare, processer och teknologier
- Inför en rutin för underrättelser om personuppgiftsincidenter, som inkluderar detektering av incidenter och responskapacitet
- Vissa organisationer måste även ha ett dataskyddsombud

PCI DSS-ramverket stödjer GDPR:s säkerhetsefterlevnad

GDPR fastställer inte i detalj ett efterlevnads-/säkerhetsramverk. Betalkortsbranschens datasäkerhetsstandard (PCI DSS) tillhandahåller dock en användbar startpunkt för efterlevnadsprogram för personuppgiftshantering. Genom att byta ut ett ord, ”kortinnehavare” till ”personuppgifter”, i de 12 huvudkraven för PCI DSS, kommer de att tillhandahålla en logisk struktur för hur man gör en strategi för säkerhetsefterlevad av GDPR:

Mål	Krav
Bygga och upprätthålla ett säkert nätverk	1. Installera och upprätthålla en brandväggskonfiguration för att skydda **personuppgifter** 2. Inte använda leverantörsangivna standarder för systemlösenord och andra säkerhetsparametrar
Skydda kortinnehavarens uppgifter	3. Skydda lagrade **personuppgifter** 4. Kryptera överföring av **personuppgifter** över öppna, offentliga nätverk
Använd ett program för hantering av sårbarheter	5. Använd och uppdatera regelbundet antivirusprogram eller andra program 6. Utveckla och använd säkra system och applikationer
Implementera stränga åtgärder för åtkomst-/passerkontroll	7. Begränsa åtkomsten till **personuppgifter** till de som har ett affärsbehov att känna till dem 8. Tilldela ett unikt ID till alla personer med datoråtkomst 9. Begränsa den fysiska åtkomsten till **personuppgifterna**
Övervaka och testa nätverken regelbundet	10. Spåra och övervaka all åtkomst till nätverksresurser och **personuppgifter** 11. Testa säkerhetssystem och -processer regelbundet
Implementera en informationssäkerhetspolicy	12. Implementera en policy om informationssäkerhet som gäller all personal

Om du följer PCI DSS och behandlar alla dina personuppgifter/viktiga uppgifter på samma sätt som du behandlar kortinnehavares uppgifter är du på rätt spår. Det som är viktigt att tänka på är att PCI DSS inte omfattar allt som fastställs i GDPR, men det är en bra startpunkt för att uppnå datasäkerhet (Artikel 32 i EU:s allmänna dataskyddsförordning, ”Säkerhet i samband med behandlingen”).

Checklista för att förbereda sig på GDPR-efterlevnad

- ☐ Inför ett arbetsprogram för att samla in en koherent inventering av dina processer som rör personuppgifter.
- ☐ Använd en process för att riskbedöma dina egna uppgifter.
- ☐ Ha förståelse för var och hur du delar personuppgifter med tredje parter och se till att du har rätt avtal på plats för att följa GDPR.
- ☐ Bedöm dina informationssäkerhetsprogram som berör personuppgifter, inklusive vilka tredje parter du delar uppgifter med.
- ☐ Följ betalkortsbranschens datasäkerhetsstandard (PCI DSS) för en grundläggande säkerhet kring personuppgifter och kortinnehavaruppgifter.
- ☐ Om tillämpligt, se till att informationen och de samtyckestexter du skickar till dina kunder är öppna, tydliga, entydiga och skrivna på ett enkelt språk.
- ☐ Fastställ en plan för efterlevnad av mer komplexa rättigheter som rör den registrerade, såsom rätt till åtkomst, korrigering, rättelse, dataportabilitet och radering.
- ☐ Inför en mekanism för att identifiera om, när och var eventuella incidenter inträffar och hur du ska hantera dem.
- ☐ Anlita en PCI Forensic Investigator (PFI) som man kan kontakta vid eventuella kortuppgiftsincidenter.

Vilka konsekvenser kan bristande efterlevnad ge?

Företag som inte har vidtagit några åtgärder för att garantera att deras personuppgiftsbehandling uppfyller de nya kraven under GDPR, kan få böter för bristande efterlevnad. Dessa böter kan ges till både personuppgiftsansvariga och personuppgiftsbiträden.

Underlåtelse att efterleva GDPR kan resultera i böter på upp till 20 miljoner euro eller 4 procent av ett företags globala omsättning, en siffra som för vissa kan innebär ett bötesbelopp på flera miljoner.

Böterna beror på hur allvarlig överträdelsen är och om företaget bedöms ha tagit efterlevnaden och bestämmelserna om säkerheten på ett tillräckligt allvarligt sätt eller inte.

Maxbeloppet för böter är 20 miljoner eller 4 procent av företagets globala omsättning, beroende på vilken summa som är högre, för överträdelse av den registrerades rättigheter, obehörig internationell överföring av personuppgifter och underlåtelse att införa procedurer för eller ignorera begäranden av den registrerade att få åtkomst till sina uppgifter.

Den lägsta gränsen på 10 miljoner euro eller 2 procent av den globala omsättningen kommer att tillämpas på företag som hanterar uppgifter felaktigt på andra sätt.
Det kan inkludera, men begränsas inte till, att underlåta att rapportera om en dataöverträdelse, underlåtelse att bygga in dataskydd och att garantera att dataskydd gäller i ett projekts första skede och att underlåta att utse ett dataskyddsombud (om tillämpligt).

Hur kan Elavon hjälpa till?

Frågor som du kan ställas inför:

- Hur får vi samtycke från våra medarbetare?
- Exakt vad är det jag behöver komma ihåg gällande behandlingsaktiviteter?
- Är vi personuppgiftsansvariga för de anställningsuppgifter vi skickar till företag som hanterar pensions- och sjukvårdsförmåner?
- Hur passar PCI DSS in i allt det här och vilken nytta kan vi ha av dem?
- Behöver vi ett dataskyddsombud?
- Vad ska vi göra med alla våra marknadsföringsuppgifter?

För att hjälpa våra kunder med dessa frågor har Elavon börjat samarbeta med ett antal ledande datasäkerhetsföretag. Tillsammans med våra partner, kan Elavon hjälpa dig att lösa alla dina PCI- och GDPR-frågor, med tjänster som sträcker sig från revisioner, konsultationer, gap-analyser och planering för incidenthantering och hanterade säkerhetstjänster och virtuella dataskyddsombud.

Kontakta oss nu på **kundservice@elavon.com** för mer information.

Låt oss samarbeta

Kontakta oss för att se hur vi kan hjälpa dig att förbereda dig inför efterlevnaden av PCI DSS och GDPR.

Vi gör det möjligt. **Du får det att hända.**

kundservice@elavon.com

+46 (0)8 593 664 67 **www.elavon.se**

Elavon Financial Services DAC Norway Branch - Organisationsnummer 991 283 900.
Besöksadress: Karenlyst Allé 11, 0278 Oslo; Postadress: Postboks 354 Skøyen, 0213 Oslo, Norge.
Huvudkontor: Elavon Financial Services DAC, Irländskt organisationsnummer 418442, Besöksadress: Building 8, Cherrywood Business Park, Loughlinstown, Co. Dublin, D18 W319 Irland.
Elavon Financial Services DAC, verksamt som Elavon Merchant Services, regleras av Irländska Centralbanken.