Faktablad om informationssäkerhet

Efterlevnad av den allmänna data-skyddsförordningen

Introduktion till informationssäkerhet

SHARP
Be Original.

www.sharp.se

Innehåll

Introduktion

Varje modernt företag står inför utmaningar när det gäller efterlevnad av den allmänna dataskyddsförordningen, speciellt när det gäller skydd av personuppgifter.

Den allmänna dataskyddsförordningen (GDPR) innebär flera utmaningar för företag över hela Europa och globalt.

Även om den allmänna dataskyddsförordningens fokus i hög grad är att skydda onlinedata omfattar den också företagens sätt att arbeta med och lagra data. Detta innebär att företagen måste beakta vad som händer med information som de registrerar (via scanning eller andra indata), lagrar, behandlar, delar, skriver ut, kopierar, faxar och arkiverar.

Förordningen omfattar kategorier såsom personuppgifter, dataskydd, rätt att bli bortglömd, personuppgiftsbiträden, personuppgiftsansvariga, personuppgiftsombud, regelefterlevnad, dataskyddsmyndighet med flera (se GDPR-ordlistan på sidan 9).

Det finns många publikationer om tolkningen av terminologin i den allmänna dataskyddsförordningen, vilka som påverkas och hur förordningen ska införlivas i företagen. Emellertid finns endast ett fåtal dokument, artiklar eller faktablad om hur den allmänna dataskyddsförordningen ska överföras till företagens språkbruk och alla processer som är kopplade till verksamheten, speciellt de som är relaterade till personuppgifter.

Genom att koppla samman företagsanvändare (anställda), affärsprocesser (arbetsflöden och bästa praxis) och affärstillgångar (hårdvara och mjukvara) har Sharp definierat tre separerade områden avseende affärssäkerhet som, när de kopplas ihop, kan förbättra företagens övergripande säkerhet så att den allmänna dataskyddsförordningen efterlevs.
Dessa tre områden är:

- **Nätverkssäkerhet**
  Avser alla typer av nätverk i en organisation som administreras av en IT-avdelning eller IT-administratör, med speciellt fokus på säkerheten för all ansluten kringutrustning för utskrift, scanning och faxning.

- **Utskriftssäkerhet**
  Avser både utskrift och scanning från multifunktionssystem eller skrivare. Avser utskrift av dokument och digitala kopior av utskrifter som överförs från en dator till en skrivare (inklusive via en skrivarserver), scanning (inklusive scanning till mapp, scanning till e-post och scanning till molntjänst) och faxning.

- **Dokumentsäkerhet**
  Avser både information som scannas från pappersdokument och digitala kopior av dokument lagrade i dokumentlager såsom e-post, digitala filer, formulär etc.

Sharp kan underlätta för företag att efterleva den allmänna dataskyddsförordningen med hjälp av verktyg och effektiva rutiner för företagets affärsprocesser som är direkt kopplade direkt till nätverks-, utskrifts- och dokumentsäkerhet.

Bakgrund

Den allmänna dataskyddsförordningen är den största förändringen inom datasäkerhet på mer än 20 år. Men många frågor kvarstår – delvis obesvarade.

Med den allmänna dataskyddsförordningen följer nya krav och ekonomiska påföljder om företaget inte har infört tillräckliga skydd och förebyggande åtgärder mot incidenter[1]. Emellertid är riktlinjerna mycket bristfälliga för vad företagare, IT-chefer och användare behöver göra för att efterleva den allmänna dataskyddsförordningen. Varje företag måste själva tolka vad som krävs av dem.

Det huvudsakliga syftet med den allmänna dataskyddsförordningen är bättre hantering och skydd vid hantering av personuppgifter. Detta innebär att alla personuppgifter i företagets affärssystem – från kund- och affärskontaktdata lagrade i mjukvaror, tillämpningar, nätverksinställningar, dokumenthanteringstillämpningar och utskriftshanteringskonton till personaldokumentation – ska hanteras på ett lämpligt sätt.

Efterlevnad av den allmänna dataskyddsförordningen inbegriper två olika nivåer:

- **Personnivå**
  Allt som rör användaren, inklusive beteende, arbetssätt och hur affärssystem och regelverk tillämpas på dem.

- **Organisationsnivå**
  Affärsprocesser inom organisationen (inklusive pappersbaserade och digitala arbetsflöden), resurser (inklusive sådana som underlättar digital och pappersbaserad delning och kommunikation), företagskultur och hur den relaterar till marknadsutmaningar.

Genom att införa strategier och verktyg på organisationsnivå kan användarna motiveras till ett förändrat beteende och arbetssätt och erfordrad hantering av alla tillgängliga företagsdata, samt att strategierna och verktygen kan övervaka denna efterlevnad. Detta leder till en bättre förståelse av hur dokument och personuppgifter ska hanteras[2].

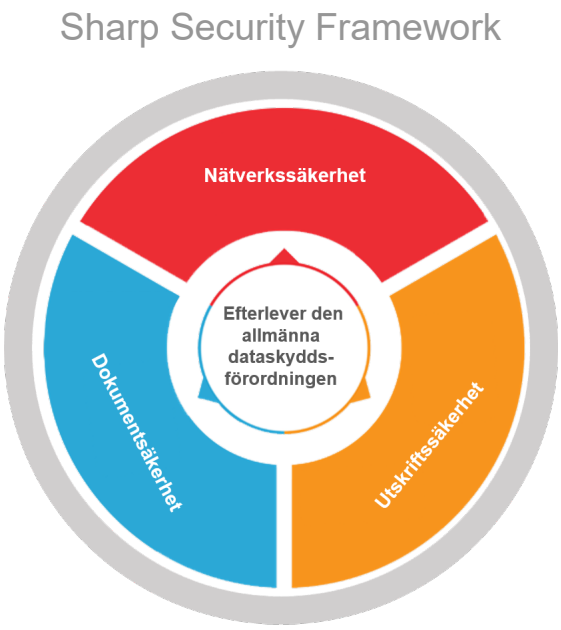
Sharp inriktar sig därför på organisationsnivån (processer, lösningar och hårdvara) och kan bidra till utformning av en grundläggande säkerhetspolicy som är avgörande för alla företag.

Vi har identifierat tre säkerhetsområden med relaterade potentiella risker som, om dessa inte hanteras, kan leda till brott mot gällande regelverk:

- **Nätverksrelaterade risker**
  - Risker i samband med konvertering av data mellan pappersdokument och digitala format och tillbaka till utskrift på papper.
  - Det är nödvändigt att multifunktionssystem och skrivare har lika hög säkerhetsnivå som hos servrar, och att en policy för genomtänkt, enhetlig utskriftssäkerhet utarbetas.
  - Enheterna måste övervakas och administreras så att säkerhetspolicyn vid behov kan upprätthållas och uppdateras när nya risker aktualiseras.
  - Data måste vid behov kunna rensas på ett säkert sätt.

- **Utskriftsrelaterade risker**
  - Behörigheter för multifunktionssystem och skrivare för övervakning av utskrift och dirigering av konfidentiella data.
  - Hantering av ett stort antal utdatatyper – kopior, utskrifter, fax, scanningfiler (inklusive scanning till e-post och scanning till mapp).
  - Spårningsinformation och redovisning av vad som har scannats eller skrivits ut.

- **Dokumentrelaterade risker**
  - Brist på definition av och förståelse för dokumentets livscykel i verksamheten. Detta inkluderar alla faser i dokumentets livscykel; från skapande till rensning av data.
  - Ostrukturerade dokumentlager som lämnar dokumenthanteringssystem öppna för attacker och potentiella incidenter.
  - Återkommande manuella uppgifter kopplade till digitala och pappersbaserade dokument, där incidenter kan inträffa till följd av att fel destination specificeras av misstag.
  - Okontrollerad delning av affärskritiska dokument.
  - Risk för dataförluster till följd av saknad versionskontroll.



Rekommendationer

Tack vare en djupgående syn på säkerhet i företag kan Sharp säkerställa efterlevnad av stränga regelverk och skapa lösningar som gör företag effektivare.

Sharp strävar efter efterlevnad av den allmänna dataskyddsförordningen inom alla områden av informationssäkerhet genom fokusering på de tre huvudområdena inom affärssäkerhet: nätverkssäkerhet, utskriftssäkerhet och dokumentsäkerhet. Med vår omfattande portfölj av optimerade produkter och lösningar samt relaterade Sharp Professional Services täcker vi in de organisatoriska aspekterna av databehandling och datasäkerhet.

Med en tydlig och enhetlig policy på verksamhetens organisationsnivå kan vi påverka användarnas beteende. I kombination med våra noggrant utarbetade och säkra system kan företag därmed efterleva den allmänna dataskyddsförordningen, samt få tillgång till effektiva verktyg för att mäta risk, förhindra cyberattacker och få mer kunskap om användarrelaterade aktiviteter.

Sharp Professional Services inrymmer alla aspekter av datasäkerhet, inklusive hur personuppgifter hanteras i affärssystem, vilket gör att företaget lättare kan efterleva den allmänna dataskyddsförordningen.

I nedanstående tabell visas en sammanfattning av hur Sharp kan hjälpa till att säkerställa företagets efterlevnad av den allmänna dataskyddsförordningen:

Den allmänna dataskyddsförordningen och Sharps lösningar och tjänster		
Säkerhetsområde	Produkter och lösningar	Efterlevnad via
Nätverkssäkerhet	• Sharp-multifunktionssystem • Sharp-skrivare • Sharp Remote Device Manager	• Behörighetsinställningar • Portbaserad behörighet • Protokollbaserad behörighet • Nätverksbaserad behörighet • Datakryptering • Dataöverskrivning
Utskriftssäkerhet	• Job Accounting II • SafeQ • Drivve Image • Prism ScanPath	• Behörighetsinställningar • Funktionsbegränsningar • Loggning och spårningsinformation • Arkivering och redigering av loggar
Dokumentsäkerhet	• Cloud Portal Office • Drivve DM • Drivve Image • Prism ScanPath	• Databasbehörighet • Behörighetskontroll • Versionskontroll • Spårbarhet • Dokumentarkivering och dokumentradering • Spårningsinformation

Slutsats

Sharp kan hjälpa företag att efterleva den allmänna dataskyddsförordningen genom införande av effektiva säkerhetsåtgärder och styrningsmetoder.

Att förstå, planera, konfigurera och införa de åtgärder och funktioner som krävs för att efterleva den allmänna dataskyddsförordningen kan vara mycket tidskrävande och orsaka stora svårigheter vid genomförandet, speciellt då inget företag är det andra likt.

Sharp rekommenderar att varje företagschef och IT-chef drar nytta av faktabladen i vårt bibliotek för vägledning om nätverkssäkerhet, utskriftssäkerhet och dokumentsäkerhet: https://www.sharp.se/cps/rde/xchg/se/hs.xsl/-/html/skydda-din-information.htm

Faktabladen innehåller fakta om risker och lösningar, samt information om:

- Sharps säkra nätverksanslutna utrustningar
- Sharps säkerhetsmjukvara som skyddar scannad och utskriven affärsinformation
- Sharps säkerhetsmjukvara som skyddar digitala dokument

Dessutom kan Sharp Professional Services-teamet hjälpa till att skapa robusta säkerhetsåtgärder och erbjuda konsulttjänster och verktyg anpassade för den aktuella verksamhetens typ och behov.

För att undvika potentiella risker inom andra områden av organisationen kan vi även hjälpa till att höja den generella säkerhetsnivån med verktyg och tjänster från Sharps portfölj:

- Nätverkssäkerhet
- Utskriftssäkerhet
- Dokumentsäkerhet
- Efterlevnad av den allmänna dataskyddsförordningen.

GDPR-ordlista[3]

Ansvarsskyldighet – den personuppgiftsansvarige är ansvarig för att den allmänna dataskyddsförordningen efterlevs, och måste dessutom kunna redovisa vilka åtgärder företaget har vidtagit för att säkerställa efterlevnad.

Incident – oavsiktlig eller olaglig destruktion, förlust, modifiering, eller obehörig spridning eller åtkomst av personuppgifter.

Personuppgiftsansvarig – den juridiska person, myndighet, organisation eller annat organ som ensam eller i samverkan med annan part avgör syfte och metod för behandling av personuppgifter.

Rätt att bli bortglömd (eller rätt att bli glömd) – varje persons rätt att få kränkande eller genant information om henne själv avlägsnad från Internet.

Personuppgiftsbiträde – "hantering" innebär varje typ av åtgärd som utförs på personuppgifter, oavsett om den är automatiserad eller utförs manuellt. Behandlingen kan bestå av insamling, registrering, organisering, användning, strukturering, lagring, anpassning, hämtning, konsulterande, destruktion med mera. Personuppgiftsbiträdet kan vara en organisation eller tredjepartsleverantör som behandlar personuppgifter för den personuppgiftsansvariges räkning. Personuppgiftsbiträdet måste följa vissa bestämda riktlinjer, ansvarar helt och hållet för hanteringen av personuppgifterna och är ansvarig i händelse av en incident.

Datainspektionen – den svenska myndighet som övervakar användningen av personuppgifter.

Personuppgiftsombud (dataskyddsombud) – person som är utsedd att övervaka att en organisation efterlever den allmänna dataskyddsförordningen.

Registrerad – person vars personuppgifter behandlas av en personuppgiftsansvarig eller ett personuppgiftsbiträde.

Personuppgifter – direkt eller indirekt information relaterad till en fysisk person, och som kan användas för att identifiera personen. Detta inkluderar namn, personnummer, platsinformation eller en online-identifierare.

Behandla – allt som kan göras med personuppgifter, från initial insamling till slutlig förstöring. Detta inkluderar organisering, modifiering, konsultering, användning, spridning, kombinering och innehav av data, digitalt eller manuellt.

Referenser

1. “UK firms could face £122bn in data breach fines in 2018”, ComputerWeekly, oktober 2016
2. “CEO Survey”, PwC, 2017
3. “GDPR Glossary of Key Terms”, High Speed Training, februari 2018

SHARP

Be Original.