Hvidbog om informationssikkerhed

Overholdelse af GDPR

En introduktion til informationssikkerhed

www.sharp.dk

SHARP
Be Original.

Indhold

Indledning

Alle moderne virksomheder står over udfordringer, når det kommer til at sikre overholdelse af EU's generelle forordning om databeskyttelse (GDPR), særligt hvad angår beskyttelse af personlige data.

Den generelle forordning om databeskyttelse (GDPR) har medført adskillige udfordringer for virksomheder på tværs af Europa og globalt.

Mens meget af GDPR fokuserer på beskyttelse af online data, så regulerer den også, hvordan virksomheder arbejder med og lagrer dataene, hvilket betyder, at de skal overveje, hvad der sker med oplysninger, de registrerer (gennem scanning eller elektronisk input), lagrer og opbevarer, behandler, deler, udskriver, kopierer, faxer og arkiverer.

Forordningen introducerer kategorier som f.eks. personlige identificerbare data, databeskyttelse, datasletning, databehandlere, dataansvarlige, databeskyttelsesansvarlige, overholdelse, databeskyttelsesmyndighed m.m.(se GDPR-ordlisten på side 9).

Der er mange publikationer, der fokuserer på, hvordan GDPR's ordlyd skal fortolkes, hvem der vil blive påvirket, og hvordan denne lovgivning skal introduceres i virksomheden. Der er dog kun et lille antal dokumenter, artikler eller hvidbøger om, hvordan GDPR skal oversættes til reelt virksomhedssprog og alle de processer, der er forbundet med virksomhedsaktiviteter – særligt dem, der er forbundet med personlige data.

Ved at forbinde virksomhedsbrugere (medarbejdere), virksomhedsprocesser (arbejdsgange og anbefalede fremgangsmåder) og virksomhedsaktiver (hardware og software) har Sharp defineret tre separate områder af virksomhedssikkerhed, der – når de sammensættes – kan forbedre generel virksomhedssikkerhed for at levere overholdelse af GDPR.

Disse tre områder er:

- **Netværkssikkerhed**
  Vedrører ethvert netværk, der anvendes af en virksomhedsorganisation, vedligeholdes af en IT-afdeling, hvor der er lagt vægt på alle tilsluttede enheder til udskrivning, scanning og faxning.

- **Printsikkerhed**
  Vedrører både udskrevet og scannet udkast fra multifunktionssystemer eller printere. Denne kategori inkluderer trykte dokumenter i papirformat og billeder af dokumenter i transit fra en computer til en udskrivningsenhed (herunder gennem dedikerede udskriftsservere), scanning (herunder scanning til mappe, scanning til e-mail, scanning til sky) og fax.

- **Dokumentsikkerhed**
  Vedrører information registreret fra papirdokumenter gennem scanningsprocessen eller elektroniske billeder af dokumenterne, der er lagret på virksomhedslagre, f.eks. e-mails, elektroniske filer, formularer osv.

Sharp kan hjælpe virksomheder med at opnå overholdelse af GDPR ved at introducere og anvende en række værktøjer og anbefalede fremgangsmåder til virksomhedsprocesser, der er direkte tilknyttet netværks-, print- og dokumentsikkerhed.

Baggrund

GDPR er den største ændring inden for databeskyttelse i mere end 20 år. Men der er stadigvæk mange spørgsmål – og begrænsede svar.

GDPR introducerer nye krav og definerer de finansielle bøder ved ikke at have tilstrækkelig beskyttelse og forebyggende foranstaltninger til at beskytte mod brud[1]. Med der gives meget begrænset vejledning om, hvad virksomhedsejere, IT-administratorer og brugere skal indføre for at overholde bestemmelserne. Det er op til hver enkelt virksomhed at fortolke det, der skal iværksættes.

Hovedformålet med at introducere GDPR var bedre at kunne administrere og beskytte behandlingen af personlige, identificerbare data. Det betyder, at alle personlige oplysninger i dine virksomhedssystemer – fra kunde- og virksomhedskontaktdata lagret i virksomhedsapplikationer til alle netværksindstillinger, dokumentadministration og udskriftsadministrationskonti til HR-dokumentation vedrørende medarbejdere – skal administreres på en passende måde.

Der er to hovedlag i GDPR-overholdelsen:

- **Personligt lag**
  Alle spørgsmål vedrørende brugeren, herunder dennes adfærd, arbejdsmåde samt hvordan virksomhedssystemer og regler gælder for dem

- **Organisationslag**
  Virksomhedsprocesserne i en organisation (herunder papirarbejdsgange og elektroniske arbejdsgange), aktiver (inklusive dem, der hjælper folk med at dele og kommunikere på en elektronisk eller papirbaseret måde), kulturen, og hvordan den reagerer på markedsudfordringer.

Ved at introducere strategier og værktøjer på organisationsniveau kan den forventede ændring i slubbrugernes adfærd, og hvordan de arbejder og behandler alle de tilgængelige virksomhedsdata, indstilles og administreres. Det fører til en bedre forståelse af, hvordan dokumenter såvel som brugeridentificerbare data skal behandles[2].

Derfor fokuserer Sharp på organisationslaget (processer, løsninger og hardware) og kan hjælpe med at skabe omfattende sikkerhedspolitikker, der er afgørende for enhver virksomhed.

Ved at fokusere på tre områder inden for virksomhedssikkerhed har Sharp beskrevet potentielle risici, der kan føre til brud på overholdelse, hvis der ikke tages fat på dem.

- **Netværksrelaterede risici**
  - Sårbarheden ved at flytte data mellem papirformat og elektroniske formater og tilbage ud på papir.
  - Behovet for at sikre multifunktionssystemer og printere til samme niveau som servere og behovet for en planlagt og fælles politik om udskriftssikkerhed.
  - Behovet for at overvåge og administrere enheder for at bevare og opdatere sikkerhedspolitikken, hvis det er nødvendigt, i tråd med nye sårbarheder med tiden.
  - Behovet for at kassere data sikkert og til tiden.

- **Udkastrelaterede risici**
  - Behovet for at sikre adgangen til multifunktionssystemer og udskriftsenheder for at kontrollere udkast og routing af fortrolige data.
  - Administration af antal og typer af udkast – kopier, udskrifter, faxer, scanninger (herunder scanning til e-mail og scanning til mappe).
  - Behovet for et revisionsspor og ansvarlighed for, hvad der er registreret eller udskrevet.

- **Dokumentrelaterede risici**
  - Mangel på definition og forståelse af dokumentlivscyklussen i virksomheden. Dette inkluderer alle trin af virksomhedslivscyklussen – fra dokumentoprettelse til -bortskaffelse.
  - Ustrukturerede dokumentlagre, der efterlader dokumentadministrationssystemer åbne for angreb og potentielle brud.
  - Repetitive manuelle opgaver forbundet med dokumenter (elektronisk og papirformat), hvorved en forkert destination kan tilføjes ved en fejl og føre til databrud.
  - Ukontrolleret deling af virksomhedsvigtige dokumenter.
  - Risiko for datakorruption uden versionskontrol.

Sharps sikkerhedsstruktur

Anbefalinger

Ved at bruge vores omfattende tilgang til virksomhedssikkerhed kan Sharp sikre overholdelse af selv de strengeste bestemmelser og skabe løsninger, der hjælper virksomheder med at arbejde mere effektivt.

Sharp har til mål at sikre GDPR-overholdelse i ethvert aspekt af informationssikkerhed ved at tage fat på de tre hovedområder inden for virksomhedssikkerhed: netværkssikkerhed, printsikkerhed og dokumentsikkerhed. Vi dækker de organisatoriske aspekter af databehandling og databeskyttelse gennem vores omfattende portefølje af optimerede produkter og løsninger samt Sharps professionelle tjenester.

Ved at opbygge en stærk base på tværs af organisationslaget i en virksomhed kan vi påvirke slutbrugerens adfærd. Sammen med vores veldesignede og sikre systemer hjælper dette virksomheder med at overholde GDPR og leverer de rette værktøjer til at måle risici, forhindre cyberangreb og give nøjagtige brugerrelaterede indblik.

Sharps professionelle tjenester dækker ethvert aspekt af datasikkerhed, herunder håndtering af personlige identificerbare oplysninger i virksomhedssystemer, og hjælper dermed organisationer med at overholde GDPR.

Nedenstående er en opsummeret tabel, der viser, hvordan Sharp kan hjælpe dig med at overholde GDPR:

Generel forordning om databeskyttelse og Sharp		
Sikkerhedsaspekt/-område	Produkter og løsninger	Overholdelse gennem
Netværkssikkerhed	• Sharps multifunktionssystemer • Sharps printere • Sharp Remote Device Manager	• Brugeradgangskontrol • Portkontrol • Protokolkontrol • Netværkssikkerhedskontrol • Datakryptering • Dataoverskrivning
Printsikkerhed	• Job Accounting II • PaperCut MF • SafeQ • Drivve Image • Prism ScanPath	• Adgangskontrol • Funktionalitetsbegrænsninger • Datalog/revisionsrapportering • Bevarelse og redaktion af datalog
Dokumentsikkerhed	• Cloud Portal Office • Drivve DM • Docuware • Drivve Image • Prism ScanPath	• Databaseadgangskontrol • Brugerrettighedskontrol • Versionssporing • Revisionsspor • Dokumentbevaring, herunder Dokumentbortskaffelse • Revisionslog

Konklusion

Sharp kan hjælpe organisationer med at etablere effektive sikkerhedsforanstaltninger og effektive administrationsmetodologier som hjælp til at opnå overholdelse af GDPR.

At forstå, planlægge, konfigurere og udføre foranstaltningerne og funktionerne, der er nødvendige for at overholde GDPR kan tage lang tid og forårsage reelle implementeringsproblemer, særligt da alle virksomheder er forskellige.

Sharp anbefaler, at virksomhedsejere og IT-administratorer læser de hvidpapirer, der er at finde i vores bibliotek, for vejledning inden for områderne for netværkssikkerhed, printsikkerhed og dokumentsikkerhed: https://www.sharp.dk/cps/rde/xchg/dk/hs.xsl/-/html/informationssikkerhed.htm

Disse hvidbøger vil beskrive risiciene samt afbødende handlinger og introducere:

- Sharps sikre netværksenheder
- Sharps sikkerhedssoftware, der hjælper med at beskytte fangst og udkast af virksomhedsdata
- Sharps sikkerhedssoftware, der hjælper med at beskytte elektroniske dokumenter.

Derudover tilbyder teamet bag Sharps professionelle tjenester rådgivning og hjælp til at opbygge robuste sikkerhedsforanstaltninger og introducere værktøjer, der er relevante for hver enhver virksomhedstype og behov.

For at undgå potentielle sårbarheder i andre områder af din organisation kan vi også hjælpe dig med at indføre yderligere sikkerhedsforanstaltninger fra Sharp-porteføljen, så du kan levere 360-graders sikkerhedsbeskyttelse for ethvert aspekt af din virksomhed:

- Netværkssikkerhed
- Printsikkerhed
- Dokumentsikkerhed
- Overholdelse af GDPR.

GDPR-ordliste[3]

Ansvarlighed – den dataansvarlige har ansvaret for overholdelse af de nye databeskyttelsesprincipper. De skal kunne demonstrere trinnene, som virksomheden tager for at sikre overholdelse.

Databrud – enhver utilsigtet eller ulovlig ødelæggelse, tab, ændring, uautoriseret offentliggørelse eller adgang til en persons data.

Dataansvarlig – dataansvarlig (eller registeransvarlig) betyder den juridiske person, offentlige myndighed, agentur eller andet organ, der – alene eller sammen med andre – fastslår formålene og behovet for behandling af personlige data.

Datasletning– (også kendt som retten til at blive glemt) omfatter den registreredes anmodning om, at den dataansvarlige sletter dennes personlige oplysninger.

Databehandler – behandling betyder enhver handling eller række af handlinger, der foretages på personlige data eller på sæt af personlige data. Det anses for værende behandling, når disse handlinger foretages manuelt såvel som automatisk. Behandling inkluderer følgende aktiviteter: indsamling, registrering, organisering, brug, strukturering, lagring, tilpasning, hentning, konsultation, ødelæggelse m.m. Databehandleren kan være en organisation eller tredjepartsleverandør, der administrerer og behandler personlige data på vegne af den dataansvarlige. Databehandlere har specifikke juridiske forpligtelser som f.eks. at bevare personlige optegnelser og er ansvarlige i tilfælde af et databrud.

Databeskyttelsesmyndighed – den nationale myndighed, der beskytter personlige data.

Databeskyttelsesrådgiver – et udpeget individ, der arbejder for at sikre, at du implementerer og overholder de politikker og procedurer, der er fastlagt af GDPR.

Den registrerede – en person, hvis personlige data behandles af en dataansvarlig eller databehandler.

Personlige data – enhver direkte eller indirekte oplysning vedrørende en identificeret person, der kan anvendes som et middel til at identificere dem. Dette inkluderer deres navn, ID-nummer, placeringsdata eller et online identifikationsnavn.

Behandling – dette refererer til enhver aktivitet vedrørende personlige data, fra indledende fangst til den endelige destruering. Det inkluderer elektronisk eller manuel organisering, ændring, konsultation, brug af, offentliggørelse, kombinering og bevaring af dataene.

Referencer

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, februar 2018

SHARP

Be Original.