«White paper» om informasjonssikkerhet

Overholdelse av GDPR

En innføring i informasjonssikkerhet

www.sharp.no

SHARP
Be Original.

Innhold

Innledning

Alle moderne bedrifter møter utfordringer når det gjelder å sikre innfrielse av personvernforordningen (GDPR) og beskytte personlig informasjon.

Personvernforordningen (GDPR) har skapt en rekke utfordringer for bedrifter både i og utenfor Europa.

Selv om mye av fokuset ligger på beskyttelse av nettdata, gjør personvernforordningen det nødvendig for bedriftene å tenke over også hva som skjer med informasjonen de innhenter (elektronisk eller gjennom skanning), lagrer og forvalter, behandler, deler, skriver ut, kopierer, fakser og arkiverer.

Gjennom forordningen innføres kategorier som bl.a. Personlige identitetsdata, Databeskyttelse, Datasletting, Databehandlere, Datakontrollører, Personvernombud, Samsvar og Databeskyttelsesmyndighet (se GDPR-terminologi på side 9).

Det har blitt gitt ut mange publikasjoner om hvordan ordlyden i GDPR skal tydes, hvem som berøres og hvordan forordningen skal innføres i bedriftene. Derimot finnes det få dokumenter, artikler eller «white paper» som omhandler hvordan man gjør GDPR om til handelsspråk, samt prosessene som er knyttet til forretningsaktivitetene (særlig med hensyn til personinformasjon).

Ved å knytte sammen bedriftsbrukere (medarbeidere), bedriftsprosesser (arbeidsflyter og beste praksis) og bedriftsaktiva (maskin- og programvare), har Sharp definert tre adskilte områder av bedriftssikkerhet som samlet kan forbedre den generelle bedriftssikkerheten for å innfri kravene i personvernforordningen.

Disse tre områdene er:

- **Nettverkssikkerhet**
  Knyttet til alle nettverk som brukes av en bedrift og vedlikeholdes av en IT-avdeling, og der fokus ligger på utskrift, skanning og faksing fra tilkoblede perifere enheter.

- **Utdatasikkerhet**
  Knyttet til dokumentene som skrives ut eller skannes fra (multifunksjons)skrivere. Denne kategorien omfatter alle utskrevne dokumenter og bilder av dokumenter i transitt fra en datamaskin til en utskriftsenhet (herunder utskrifter gjennom egne utskriftsservere), skanning (innbefattet skanning til mapper, e-poster, skyen eller HDD) og faks.

- **Dokumentsikkerhet**
  Knyttet til informasjon fra skannede papirdokumenter eller elektroniske bilder av dokumenter som er lagret i bedriftens datasamlinger (f.eks. e-poster, elektroniske filer og skjemaer).

Sharp kan hjelpe bedriftene å oppfylle personvernforordningen ved å innføre og ta i bruk verktøy og beste praksiser for bedriftsprosesser som er knyttet direkte til nettverks-, utdata- og dokumentsikkerhet.

Bakgrunn

Personvernforordningen (GDPR) er det viktigste som har hendt innenfor databeskyttelse på mer enn 20 år. Spørsmålene er imidlertid fortsatt mange – og svarene begrenset.

Personvernforordningen innfører nye krav og bøtelegging ved utilstrekkelig bruk av forebyggende tiltak mot brudd på persondatasikkerheten[1]. Dessverre går man i svært liten grad inn på hva bedriftseiere, IT-ansvarlige og brukere trenger å gjøre for å innfri forordningen. Hver bedrift må selv avgjøre hvilke tiltak som er nødvendige.

Det primære målet med personvernforordningen er å administrere og beskytte behandlingen av personopplysninger på en bedre måte. Dette innebærer at alle personopplysninger i bedriftssystemene – fra forretnings- og kundekontaktinformasjon som er lagret i bedriftsprogrammene, til nettverksinnstillinger, dokument- og utskriftsstyringskontoer samt HR-dokumentasjon om personale – må administreres på en forsvarlig måte.

Vi skiller mellom to hovednivåer av GDPR-samsvar:

- **Personlig nivå**
  Alt som gjelder brukerne – innbefattet brukeratferd, arbeidsmåte og hvordan de berøres av bedriftssystemer og -prosesser.

- **Organisasjonsnivå**
  Forretningsprosessene i en organisasjon (innbefattet papirbaserte og elektroniske arbeidsflyter), aktiva (herunder aktivaene som muliggjør deling og kommunikasjon enten elektronisk eller på papir), kultur og respons på markedsutfordringer.

Ved å innføre strategier og verktøy på organisasjonsnivå kan man angi og styre hvordan sluttbrukerne skal arbeide med og behandle de tilgjengelige bedriftsdataene. Dette gir en økt innsikt i hvordan dokumenter og personidentifiserbare data skal behandles[2].

Sharp fokuserer derfor på organisasjonsnivået (prosesser, løsninger og maskinvare), og kan hjelpe med å utarbeide de omfattende sikkerhetsretningslinjene som dagens bedrifter er helt nødt til å ha.

Sharp har definert tre kjerneområder av bedriftssikkerhet og undersøkt risikoer som her kan føre til brudd på persondatasikkerheten:

- **Nettverksrelaterte risikoer**
  - Sårbarhetene som oppstår når man flytter data fra papirformat til elektronisk format og så tilbake til papir.
  - Viktigheten av å gi (multifunksjons)skrivere samme sikkerhetsnivå som servere, og behovet for gjennomtenkte og konsekvente retningslinjer for utskriftssikkerhet.
  - Behovet for å overvåke og administrere enheter for å håndheve sikkerhetsretningslinjene og oppdatere dem etter hvert som det oppstår nye sårbarheter.
  - Behovet for å destruere data på en sikker måte innen rimelig tid.

- **Utdatarelaterte risikoer**
  - Behovet for å sikre tilgangen til multifunksjonsskrivere og utskriftsenheter for å ha kontroll med utdata samt ruting av konfidensielle data.
  - Administreringen av antall og type kopier, utskrifter, fakser og skanninger (innbefattet skanninger til e-post og mappe).
  - Behovet for å ha et revisjonsspor og kunne gjøre rede for hva som har blitt innhentet eller skrevet ut.

- **Dokumentrelaterte risikoer**
  - Mangel på definisjon og forståelse av dokumentlivssyklusen i bedriften. Dette

innbefatter samtlige trinn i dokumentlivssyklusen, fra dokumentet opprettes og til det destrueres.
- Ustrukturerte datasamlinger som gjør dokumentadministrasjonssystemene sårbare for angrep og potensielle brudd på persondatasikkerheten.
- Manuelle rutineoppgaver knyttet til dokumenter (i elektronisk eller papirformat), der det ved en feiltakelse kan bli angitt feil destinasjon og dermed oppstå brudd på persondatasikkerheten.
- Ikke-kontrollert deling av forretningskritiske dokumenter.
- Risiko for ødelagte datafiler uten versjonskontroll.

Sikkerhetsrammeverk fra Sharp

Anbefalinger

Gjennom en omfattende tilnærming til bedriftssikkerhet kan Sharp hjelpe bedrifter å innfri selv de strengeste forskriftene og jobbe mer effektivt.

Sharps mål er å sikre samsvar med personvernforordningen i alt som angår informasjonssikkerhet, ved å gripe an de tre kjerneområdene nettverks-, utdata- og dokumentsikkerhet. Vår rikholdige portefølje av optimaliserte produkter og løsninger samt relaterte profesjonelle tjenester dekker samtlige organisatoriske aspekter ved databehandling og -beskyttelse.

Ved å skape et sterkt grunnlag på organisasjonsnivå i bedriften kan vi påvirke sluttbrukernes atferd. Kombinert med våre gjennomtenkte og sikre systemer vil dette hjelpe bedriftene å innfri personvernforordningen, gi egnede verktøy for måling av risiko og forebygging av cyberangrep, og levere nøyaktig brukerrelatert innsikt.

Sharps profesjonelle tjenester omfatter alle aspekter ved datasikkerheten – innbefattet hvordan personidentifiserbar informasjon håndteres i bedriftssystemene – slik at organisasjonene enklere kan oppfylle kravene i personvernforordningen.

Tabellen under viser i korte trekk hvordan Sharp kan hjelpe deg å innfri personvernforordningen:

Personvernforordningen (GDPR) og Sharp		
Sikkerhetsaspekt/-område	Produkter og løsninger	Samsvar gjennom
Nettverkssikkerhet	• Multifunksjonsskrivere fra Sharp • Skrivere fra Sharp • Sharp Remote Device Manager	• Kontroll av brukertilgang • Portkontroll • Protokollkontroll • Kontroll av nettverkstjenester • Kryptering av data • Overskriving av data
Utdatasikkerhet	• Job Accounting II • PaperCut MF • SafeQ • Drivve Image • Prism ScanPath	• Tilgangskontroll • Funksjonsbegrensninger • Datalogg/ revisjonsrapportering • Lagring og redigering av datalogger
Dokumentsikkerhet	• Cloud Portal Office • Drivve DM • Docuware • Drivve Image • Prism ScanPath	• Kontroll av databasetilgang • Kontroll av brukerrettigheter • Versjonssporing • Revisjonsspor • Dokumentlagring inkl. destruering av dokumenter • Revisjonslogg

Konklusjon

Sharp kan hjelpe organisasjoner å implementere effektive sikkerhetstiltak og styringsmetoder som bidrar til å sikre innfrielse av kravene i personvernforordningen.

Særlig ettersom alle bedrifter er forskjellige, kan det å skulle skaffe seg innsikt i, planlegge, konfigurere og utføre tiltakene og funksjonene som kreves for å innfri personvernforordningen, være en tidkrevende prosess og by på store implementeringsutfordringer.

Sharp anbefaler at bedriftseiere og IT-ansvarlige besøker «white paper»-biblioteket vårt for å sette seg mer inn i nettverks-, utdata- og dokumentsikkerhet: https://www.sharp.no/cps/rde/xchg/no/hs.xsl/-/html/informasjonssikkerhet.htm

I tillegg til en beskrivelse av risikoer og løsningstiltak finner du her en presentasjon av:

- Sikre nettverksenheter fra Sharp
- Sikkerhetsprogramvare fra Sharp som er med på å beskytte dataene som bedriften innhenter og produserer
- Sikkerhetsprogramvare fra Sharp som er med på å beskytte elektroniske dokumenter

Sharps profesjonelle serviceteam tilbyr dessuten rådgivning samt hjelp til å iverksette effektive sikkerhetstiltak og ta i bruk verktøy som er relevante for bedriftens konkrete behov.

For at du skal unngå potensielle svakheter på andre områder i organisasjonen din, kan vi også hjelpe deg å innføre ytterligere sikkerhetstiltak fra Sharp-porteføljen. På den måten kan du sørge for at hvert eneste aspekt av virksomheten beskyttes fullt ut:

- Nettverkssikkerhet
- Utdatasikkerhet
- Dokumentsikkerhet
- Samsvar med personvernforordningen

GDPR-terminologi[3]

Ansvar – datakontrolløren er ansvarlig for at prinsippene for databeskyttelse innfris. Vedkommende må kunne dokumentere tiltakene som bedriften tar for å sikre forskriftssamsvar.

Brudd på persondatasikkerheten – utilsiktet eller lovstridig ødeleggelse, tap, endring, utlevering av eller tilgang til personopplysninger.

Datakontrollør – dette er en juridisk person, en offentlig myndighet, et byrå eller en annen instans som – alene eller i samarbeid med andre – avgjør hvordan og for hvilke formål personopplysninger skal behandles.

Datasletting– er retten som datasubjektene har til å kreve at datakontrolløren sletter personopplysningene deres.

Databehandler – «behandling» omfatter all håndtering av personopplysninger. Det regnes som behandling uansett om håndteringen utføres automatisk eller manuelt. Behandling omfatter blant annet følgende aktiviteter: innsamling, registrering, organisering, bruk, strukturering, lagring, tilpassing, innhenting, oppslag og destruering. Databehandleren kan være en organisasjon eller tredjepartsleverandør som administrerer og behandler personopplysninger på vegne av kontrolløren. Databehandlerne har lovpålagte forpliktelser som f.eks. føring av personaljournaler, og stilles til ansvar ved brudd på persondatasikkerheten.

Databeskyttende myndighet – den nasjonale myndigheten som beskytter personvernet.

Personombud – en utnevnt person som jobber med å sikre at du bruker og følger retningslinjene og prosedyrene som personvernforordningen krever.

Datasubjekt – vedkommende som får personopplysningene sine behandlet av en kontrollør eller behandler.

Personopplysninger – personinformasjon som muliggjør direkte eller indirekte identifisering av en person. Dette innbefatter navn, ID-nummer, stedsinformasjon eller nettbaserte identifikatorer.

Behandling – all personopplysningsrelatert aktivitet fra personopplysningene samles inn og til de destrueres. Dette innbefatter sortering, endring, oppslag, bruk, utlevering, kombinering og lagring av data enten elektronisk eller manuelt.

Referanser

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.